UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-003-9

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

December 6, 2022

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-003-9

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] the North American Electric Reliability Corporation ("NERC")[3] hereby submits for Commission approval proposed Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls. The proposed Reliability Standard addresses supply chain risk management for assets containing low impact Bulk Electric System ("BES") Cyber Systems. NERC requests that the Commission approve the proposed Reliability Standard, provided in Exhibit A hereto, as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

NERC also requests approval of:

- the associated Implementation Plan (Exhibit B);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and D); and

[1] 16 U.S.C. § 824o.
[2] 18 C.F.R. § 39.5 (2022).
[3] The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp*., 116 FERC ¶ 61,062 (2006), *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

- the retirement of Commission-approved Reliability Standard CIP-003-8.

As required by Section 39.5(a) of the Commission's regulations,[4] this petition presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history and complete record of development (Exhibit G), and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672[5] (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on November 16, 2022.

I. SUMMARY

Entities' increasing reliance on microprocessor-driven devices to operate the BES introduces cyber security supply chain risks.[6] These devices help entities to have better responsive control over BES equipment but also, if compromised through supply chain vulnerabilities, could impact BES reliability. As such, NERC's cyber security Critical Infrastructure Protection ("CIP") Reliability Standards seek to mitigate cyber security risks, including supply chain risks, to BES Facilities, systems, and equipment. To address these risks, the cyber security CIP standards focus on protections around BES Cyber Systems located at or associated with BES Facilities, systems, and equipment. Responsible Entities[7] categorize BES Cyber Systems as low, medium, or high impact based on the characteristics of their BES Facilities, systems, and equipment. Depending on the assigned impact level, Responsible Entities then apply corresponding requirements from the

---

4 18 C.F.R. § 39.5(a).

5 The Commission specified in Order No. 672 certain general factors it would consider when assessing whether a particular Reliability Standard is just and reasonable. *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, at P 262, 321-37 ("Order No. 672"), *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

6 NERC, *State of Reliability Report* at p. 60 (July 2022), https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2022.pdf.

7 As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

CIP Reliability Standards to their BES Cyber Systems or the assets containing those BES Cyber Systems.

Since the development of the original Supply Chain Standards,[8] NERC has continued to focus on supply chain risk management as it relates to the reliability of the Bulk Power System ("BPS"). In addition to Reliability Standards requirements, NERC has leveraged several tools to address these risks, including NERC Alerts, a joint white paper with FERC staff,[9] and an initiative dedicated to supply chain risk mitigation, among other activities. As part of this continued focus on supply chain issues, NERC conducted a study to evaluate supply chain risks associated with assets containing low impact BES Cyber Systems[10] (Exhibit E-1) and collected data to assess whether further revisions to the CIP Reliability Standards were needed to address these risks. Based on the data collected, NERC determined that low impact BES Cyber Systems, while still low impact to the BES, could present a greater risk if numerous assets were compromised through remote access. To that end, NERC recommended revisions to the CIP Reliability Standards to address supply chain risk management for assets containing low impact BES Cyber Systems (Exhibit E-2).[11]

---

[8] These include CIP-005-6, CIP-010-3, and CIP-013-1, which were approved by the Commission in Order No. 850. *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018).

[9] NERC and FERC, *Joint Staff White Paper on Supply Chain Vendor Identification – Noninvasive Network Interface Controller* (July 31, 2020), at https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf.

[10] *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 17, 2019), available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf.

[11] *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (Dec. 9, 2019), available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf.

Proposed Reliability Standard CIP-003-9 requires entities to adopt and maintain cyber security policies for the areas covered under the other CIP cyber security standards. The purpose of these policies is to communicate management goals, objectives, and expectations for protecting BES Cyber Systems. Proposed Reliability Standard CIP-003-9 also contains all of the requirements applicable to low impact BES Cyber Systems. Proposed Requirement R2 of CIP-003-9 requires Responsible Entities to implement cyber security plans for low impact BES Cyber Systems that address the following areas: (1) cyber security awareness; (2) physical security; (3) electronic access; (4) Cyber Security Incident response; (5) Transient Cyber Asset and Removable Media malicious code risk mitigation; and (6) vendor electronic remote access security controls.

The revisions in proposed Reliability Standard CIP-003-9 improve upon Commission-approved CIP-003-8 by adding new requirements focused on supply chain risk management for low impact BES Cyber Systems. Proposed Requirement R1, Part 1.2.6 requires Responsible Entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies. Proposed Requirement R2, Attachment 1, Section 6 requires Responsible Entities with assets containing low impact BES Cyber Systems that have established vendor electronic remote access to have methods for determining and disabling that vendor electronic remote access as well as one or more methods for detecting malicious communications for only that vendor electronic remote access. The proposed requirements enhance reliability by requiring controls that grant Responsible Entities additional visibility into threats posed by supply chain risks to low impact BES Cyber Systems. The proposed requirements also address the risks identified in NERC assessments (Exhibit E) by requiring controls around vendor electronic remote access, a potential vector of attack into BES Cyber Systems.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[12]

Lauren Perotti*
Senior Counsel
Marisa Hecht*
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Howard Gugel*
Vice President and Director of Engineering and Standards
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
howard.gugel@nerc.net

III. BACKGROUND

The following background information is provided below: (1) an explanation of the regulatory framework for NERC; (2) a description of the NERC Reliability Standards Development Procedure; (3) an overview of the NERC Board directive to revise CIP-003-8 to address supply chain risk management for low impact BES Cyber Systems; and (4) the development history for Project 2020-03 Supply Chain Low Impact Revisions, which developed the proposed Reliability Standard addressed in this petition.

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[13] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the BPS, and with the duty of

[12] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

[13] 16 U.S.C. § 824o.

certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[14] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[15] Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[16]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the BPS and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[17]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[18] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[19]

---

14 *Id*. § 824o(b)(1).
15 *Id*. § 824o(d)(5).
16 18 C.F.R. § 39.5(a).
17 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).
18 Order No. 672 at P 334.
19 The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

In its order certifying NERC as the Commission's ERO, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards[20] and thus satisfy certain criteria for approving Reliability Standards.[21] The development process is open to any person or entity with a legitimate interest in the reliability of the BPS. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the Board is required before NERC submits the Reliability Standard to the Commission for approval.

C. NERC Board Directive to Address Supply Chain Risk Management

In 2017, the Board adopted the original Supply Chain Standards[22] applicable to medium and high impact BES Cyber Systems. Concurrently, the Board directed further study of supply chain risks associated with low impact BES Cyber Systems, among other related directives.[23] Pursuant to that directive, NERC identified supply chain risks similar to those affecting medium and high impact BES Cyber Systems, such as introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems.[24] However, individual low impact BES Cyber Systems still pose a lower risk to the BES if compromised through supply chain vectors than higher impact BES Cyber Systems.[25] As such, NERC identified the potential for a greater impact if numerous low impact BES Cyber Systems are compromised or low impact BES Cyber Systems are used to gain access to higher impact BES Cyber Systems. Due to this

---

20 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 at P 250 (2006).

21 Order No. 672, *supra* note 5, at PP 268, 270.

22 These include CIP-005-6, CIP-010-3, and CIP-013-1, which were approved by the Commission in Order No. 850. *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018).

23 NERC Board of Trustees, *Minutes* at pp. 9-10, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20August%2010%202017%20Minutes.pdf

24 Exhibit E-1 at p. 17.

25 *Id.*

potential risk, NERC recommended further study of whether additional information supports modifying Reliability Standards to apply supply chain requirements to assets containing low impact BES Cyber Systems (Exhibit E-1).[26]

Accordingly, NERC issued a request pursuant to Section 1600 of the NERC Rules of Procedure to collect data and information from registered entities. NERC analyzed the collected data and information and issued a report with recommendations in 2019 (Exhibit E-2).[27] The report found that while most low impact assets reside at organizations with higher impact assets subject to the Supply Chain Standards, these low impact assets may not receive the same protections as higher impact assets within an organization, particularly if the low impact assets use separate vendors. The report also found that while these are low impact assets, the risk of a coordinated attack among a large number of low impact assets with remote electronic access connectivity would result in an event with an interconnection-wide impact on the BES. Therefore, the report recommended revisions to the CIP Reliability Standards to apply supply chain risk management requirements to low impact assets with remote electronic access connectivity. Based on these findings and recommendations, the Board in 2020 directed initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.[28]

---

[26] *Id.* at p. 4.

[27] *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (Dec. 9, 2019), available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf.

[28] NERC Board of Trustees, *Minutes* at p. 13, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf.

D. Development of the Proposed Reliability Standard

As further described in Exhibit G hereto, NERC developed a Standard Authorization Request to address the Board directive and assigned it to the Project 2020-03 standard drafting team.[29] On August 27, 2021, NERC posted the initial draft of proposed Reliability Standard CIP-003-9 for a 45-day comment period, which included an initial ballot during the last 10 days of the comment period. The initial ballot of CIP-003-9 did not receive the requisite approval, with 29.09 percent affirmative votes and 83.28 percent quorum. On February 25, 2022, NERC posted the second draft of proposed Reliability Standard CIP-003-9 for a 50-day comment period, which included an additional ballot during the last 10 days of the comment period. The additional ballot of CIP-003-9 did not receive the requisite approval, with 52.81 percent affirmative votes and 81.51 percent quorum. On July 6, 2022, NERC posted the third draft of proposed Reliability Standard CIP-003-9 for a 45-day comment period, which included an additional ballot during the last 10 days of the comment period. The additional ballot of CIP-003-9 received the requisite approval, with 66.81 percent affirmative votes and 85.22 percent quorum. On October 26, 2022, NERC conducted a ten-day final ballot for proposed Reliability Standard CIP-003-9, which received affirmative votes of 68.95 percent of the ballot pool and 86.25 percent quorum. The Board adopted the proposed Reliability Standard on November 16, 2022.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, proposed Reliability Standard CIP-003-9 addresses the supply chain risks described in Section III.C by requiring controls for vendor electronic remote access for low impact BES Cyber Systems. Proposed CIP-003-9 enhances the cyber security posture of Responsible Entities by requiring controls around supply chain risks posed by vendor

[29] The roster for the Project 2020-03 standard drafting team is included as Exhibit H to this Petition.

electronic remote access to low impact BES Cyber Systems and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. This section discusses the modifications in the requirements of CIP-003-9 (Subsection A) and the enforceability of the proposed Reliability Standard (Subsection B).

A. Modifications in Proposed Reliability Standard CIP-003-9

Proposed Reliability Standard CIP-003-9 includes cyber security policies for the areas covered under the other CIP cyber security standards. In addition, proposed CIP-003-9 includes all the controls applicable to low impact BES Cyber Systems. The revisions in proposed CIP-003-9 contain additional requirements applicable to Responsible Entities with low impact BES Cyber Systems to mitigate the risks of vendor electronic remote access. Requirement R1, Part 1.2 includes a proposed new policy topic in Part 1.2.6. Under this requirement, Responsible Entities must include the topic of "vendor electronic remote access security controls" in their cyber security policies required under Requirement R1. Policies help to ensure management and executive personnel awareness and support of cybersecurity practices, creating a culture of security at all levels of an organization. Similar to other policies required under Part 1.2, proposed Part 1.2.6 will require CIP Senior Manager approval at least once every 15 calendar months, thereby continuing reinforcement of policies regarding vendor electronic remote access security controls.

Proposed new Section 6 of Requirement R2, Attachment 1 includes the processes that must be included in cyber security plans pursuant to Requirement R2:

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Similar to other sections in Attachment 1, proposed Section 6 applies to assets containing low impact BES Cyber Systems. Applicability is further narrowed to those assets that allow vendor electronic remote access and have established such access pursuant to the electronic access controls under Section 3.1. Focusing applicability on these assets is consistent with the recommendations in the 2019 Supply Chain Risk Assessment (Exhibit E-2) stating that permitting third-party electronic access to these locations without appropriate controls contributes to the risk of a coordinated cyber attack. Therefore, Section 6 applicability focuses on the access that most likely contributes to the risks identified in the NERC Staff Reports (Exhibit E), such as introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems.

The controls in proposed Section 6 seek to limit the ability to leverage trusted vendor access through supply chain vulnerabilities. Sections 6.1 and 6.2 are similar to the Supply Chain Standards requirements in Reliability Standard CIP-005-7, Requirement R2, Parts 2.4 and 2.5 that are applicable to medium and high impact BES Cyber Systems. Consistent with Part 2.4, Section 6.1 requires Responsible Entities to have one or more method(s) for determining vendor electronic remote access. This determination provides visibility into vendor electronic remote access should any issues arise that need attention. Different than Part 2.4, proposed Section 6 tailors the requirements to low impact BES Cyber Systems by eliminating references to the NERC Glossary term Interactive Remote Access, which incorporates concepts such as Electronic Access Points and Electronic Security Perimeters, both of which are applicable to medium and high impact BES Cyber Systems. Instead, proposed Section 6.1 focuses on the concept of vendor electronic remote

access to provide the flexibility to tailor controls to low impact BES Cyber Systems. Proposed Section 6.2 is consistent with the requirement in CIP-005-7, Requirement R2 Part 2.5 by requiring Responsible Entities have one or more methods for disabling vendor electronic remote access. Requiring Responsible Entities to have such a method would provide them the ability to prevent propagation of any further issues caused by vendor electronic remote access. Similar to Section 6.1, Section 6.2 is tailored to low impact BES Cyber Systems by focusing on vendor electronic remote access rather than any Glossary terms associated with medium and high impact BES Cyber Systems. In summary, proposed Sections 6.1 and 6.2 incorporate similar controls as those applicable to medium and high impact BES Cyber Systems but tailored to low impact BES Cyber Systems through greater flexibility. This flexibility is appropriate for low impact BES Cyber Systems given the large number of them and different types of organizations with low impact BES Cyber Systems. For example, the flexibility permits Responsible Entities with multiple impact level BES Cyber Systems to match their low controls with those applicable to medium and high while simultaneously permits small, lows-only organizations to apply controls appropriate to their organizational needs.

Proposed Section 6.3 requires Responsible Entities to have one or more methods to detect known or suspected inbound and outbound malicious communications for vendor electronic remote access. This requirement is similar to CIP-005-7, Requirement R1, Part 1.5 applicable to Electronic Access Points of high and medium impact BES Cyber Systems at Control Centers. The control provides additional visibility to Responsible Entities in identifying threats and is consistent with the recommendations of the NERC Staff Reports (Exhibit E). The standard drafting team recognized that CIP-005-7, Requirement R1, Part 1.5 is not applicable to all medium impact BES Cyber Systems. However, the application of that same requirement to vendor electronic remote

access at assets containing low impact BES Cyber Systems in Section 6.3 is risk-based. Medium impact BES Cyber Systems are required to have additional controls, such as Intermediate Systems or multi-factor authentication, to address the risks posed by malicious communications. Therefore, the application of methods to detect known or suspected malicious communications to applicable low impact BES Cyber Systems is consistent with the risk-based model, given those BES Cyber Systems are not subject to the other controls applicable to medium impact BES Cyber Systems. As a result, Responsible Entities are applying the controls commensurate with the risk of low impact BES Cyber Systems.

Furthermore, the standard drafting team determined focusing on detecting malicious communications for vendor electronic remote access is consistent with recommendations in the NERC Staff Reports (Exhibit E). NERC identified that one of the most significant risks is employees of vendors who have remote access.[30] Furthermore, NERC identified that one of the ways to reduce supply chain vulnerabilities is to limit this type of access.[31] In instances where this access must be established, the standard drafting team determined that Responsible Entities need visibility into vendor communications to appropriately react to any supply chain threat.[32] This visibility is achieved through Section 6.3 detection of malicious communications for vendor electronic remote access.

Finally, the proposed Reliability Standard includes other minor modifications to the non-enforceable sections of the standard. These changes are shown in redline in Exhibit A.

---

[30] Exhibit E-1 at p. 1 (citing American Public Power Association and National Rural Electric Cooperative Association, *Managing Cyber Supply Chain Risk – Best Practices for Small Entities* at p. 11 (April 2018), at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf).

[31] Exhibit E-2 at p. 12.

[32] The standard drafting team documented its intent in developing the revised standard in technical rationale provided in Exhibit F.

B. Enforceability of Proposed Reliability Standard

The proposed Reliability Standard also includes measures that support the requirements by clearly identifying what is required and how the ERO will enforce the requirements. The measures help ensure that the requirement will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[33] Additionally, the proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment. Exhibit D provides a detailed review of the revised VRF and VSLs, and the analysis of how the VRF and VSLs were determined using these guidelines.

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standard to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan provides that proposed CIP-003-9 shall become effective on the first day of the first calendar quarter that is 36 months after the effective date of the Commission's order approving the proposed Reliability Standard. The drafting team determined 36 months would be an appropriate implementation timeframe due to the large number of assets containing low impact BES Cyber Systems that would need to be updated and the demand for certain types of equipment that may be necessary to implement the new requirements.

For instance, Responsible Entities may need to acquire equipment such as intrusion detection systems to meet the monitoring requirements in Attachment 1, Section 6.3. Given the large number of assets containing low impact BES Cyber Systems, Responsible Entities would

[33] Order No. 672 at P 327.

likely try to acquire a large number of these systems simultaneously. In light of recent increased demand for parts such as semiconductor chips for all industries,[34] lead times on orders for these systems likely are longer than in years past. Furthermore, once acquired, the equipment needs to be installed and calibrated to perform effectively. Therefore, the drafting team determined a 36-month implementation timeframe would permit Responsible Entities to acquire these systems at the scale needed for low impact BES Cyber Systems while accommodating any supply chain delays due to high demand for similar equipment. Therefore, the proposed implementation timeframe strikes the appropriate balance of "the urgency in the need to implement [the requirements] against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability."[35]

VI. RELATED EFFORTS

Addressing the ever-evolving cybersecurity threat landscape is a longstanding focus of NERC. In addition to the proposed Reliability Standard CIP-003-9, NERC is working on other efforts related to low impact BES Cyber Systems or supply chain risk management.

A. Low Impact Criteria Review Team

In light of the SolarWinds cybersecurity event[36] and the evolving threat landscape facing Responsible Entities, the Board directed NERC Staff, working with stakeholders, to complete a review and analysis on facilities that house low impact BES Cyber Assets.[37] To assist in this

---

[34] U.S. Dept. of Energy, *Semiconductor: Supply Chain Deep Dive Assessment* at p. 5 (Feb. 24, 2022), at https://www.energy.gov/sites/default/files/2022-02/Semiconductor%20Supply%20Chain%20Report%20-%20Final.pdf (describing the growth in the semiconductor chip market).

[35] Order No. 672 at P 333.

[36] FERC and NERC Electricity Information and Analysis Sharing Center ("E-ISAC") Staff prepared a joint report on SolarWinds and Related Supply Chain Compromise. FERC and NERC E-ISAC Staff, *SolarWinds and Related Supply Chain Compromise*, available at https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf.

[37] NERC Board of Trustees, *Minutes* at p. 7, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Feb%204%202021.pdf.

review and analysis, NERC staff assembled a team of cybersecurity experts and compliance experts, including members of FERC staff, representative of a cross section of industry, called the Low Impact Criteria Review Team ("LICRT"). Specifically, the LICRT reviewed the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and assessed whether the low impact criteria should be modified. The LICRT identified coordinated cyber attack methods on low impact BES Cyber Systems, some of which are through supply chain vectors while others are unrelated to supply chain:

(1) unauthorized remote access,
(2) malicious software,
(3) supply chain common service attack,
(4) supply chain product compromise,
(5) unauthorized internal access by a single actor,
(6) denial of service attack,
(7) data manipulation, and
(8) unauthorized internal access by multiple actors.[38]

In reviewing these methods, the LICRT analyzed the CIP Reliability Standards for potential gaps and provided recommended next steps. While the LICRT did not recommend revising the low impact criteria in Reliability Standard CIP-002-5.1a, the LICRT did recommend the following standards revisions in addition to Security Guidelines and Risk Monitoring:

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

[38] NERC, *Low Impact Criteria Review Report: NERC Low Impact Criteria Review Team White Paper* at pp. 5-7 (October 2022), at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC_LICRT_White_Paper_clean.pdf.

- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.[39]

On November 16, 2022, the Board accepted the whitepaper and its recommendations. As for next steps, the LICRT will develop a Standard Authorization Request to initiate standards development for these recommended requirements. Some of these recommended protections do address supply chain risk management, but they also address the broader cyber attack methods identified by the LICRT. As such, NERC requests the Commission consider these future projects when reviewing proposed Reliability Standard CIP-003-9 for approval.

B. Project 2016-02 Standard Drafting Team

Project 2016-02 – Modifications to CIP Standards currently are addressing revisions to the CIP suite of Reliability Standards to incorporate applicable protections for virtualized environments. NERC periodically reports on the status of this project to the Commission in Docket No. RD20-2-000. While the revisions developed in Project 2016-02 do not address supply chain risk management, NERC notes that the standard drafting team plans to revise CIP-003-9 to incorporate conforming changes related to its virtualized technologies revisions across the suite of CIP Reliability Standards.

[39] *Id.* at pp. 13-15.

VII. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve:

- proposed Reliability Standard CIP-003-9, and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B; and
- the retirement of Commission-approved Reliability Standard CIP-003-8, effective as proposed herein.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

December 6, 2022

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A

Proposed Reliability Standard CIP-003-9

Proposed Reliability Standard CIP-003-9

Clean

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-9:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-9.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic	remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.

Version	Date	Action	Change Tracking
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Proposed Reliability Standard CIP-003-9

Redline

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~8~~9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~8~~9:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-9.

~~See Implementation Plan for CIP-003-8.~~

~~**6. Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;~~ and~~

1.2.6. Vendor electronic remote access security controls; and

~~**1.2.6.**~~**1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

~~1.1.~~ Compliance Enforcement Authority:

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~1.3.~~ Evidence Retention:

~~1.4.~~1.2. The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

~~**1.5. Compliance Monitoring and Assessment Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~**1.12. Additional Compliance Information:**~~

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems, but did not address one of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address two of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address three of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	four or more of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic	remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.

Version	Date	Action	Change Tracking
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

~~appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~1.1.1 Personnel and training (CIP-004)~~

- ~~Organization position on acceptable background investigations~~
- ~~Identification of possible disciplinary action for violating this policy~~
- ~~Account management~~

~~0.1.2~~ Vendor Electronic ~~Security Perimeters (CIP-005) including Interactive~~ Remote Access

- ~~Organization stance on use of wireless networks~~
- ~~Identification of acceptable authentication methods~~
- ~~Identification of trusted and untrusted resources~~
- ~~Monitoring and logging of ingress and egress at Electronic Access Points~~
- ~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~
- ~~Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~
- ~~Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access~~
- ~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~1.1.3 Physical security of BES Cyber Systems (CIP-006)~~

- ~~Strategy for protecting Cyber Assets from unauthorized physical access~~
- ~~Acceptable physical access control methods~~
- ~~Monitoring and logging of physical ingress~~

~~1.1.4 System security management (CIP-007)~~

- ~~Strategies for system hardening~~
- ~~Acceptable methods of authentication and access control~~
- ~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~
- ~~Monitoring and logging of BES Cyber Systems~~

~~1.1.5 Incident reporting and response planning (CIP-008)~~

- ~~Recognition of Cyber Security Incidents~~
- ~~Appropriate notifications upon discovery of an incident~~
- ~~Obligations to report Cyber Security Incidents~~

~~1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

- ~~Availability of spare components~~
- ~~Availability of system backups~~

~~1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

- ~~Initiation of change requests~~
- ~~Approval of changes~~
- ~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

- ~~Information access control methods~~
- ~~Notification of unauthorized information disclosure~~
- ~~Information access on a need-to-know basis~~

~~1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

- ~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~
- ~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

- ~~Method(s) for delivery of security awareness~~
- ~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

- ~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

- ~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

- ~~Recognition of Cyber Security Incidents~~

- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

~~combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Section 91.~~Section 7. ~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control.~~: Examples of ~~monitoring controls~~evidence showing the implementation of the process for Section 6 may include, but are not limited to: ~~(1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

~~Requirement R2, Attachment 1,~~ For Section **~~3 – Electronic Access Controls~~**

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing~~

low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the

~~specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

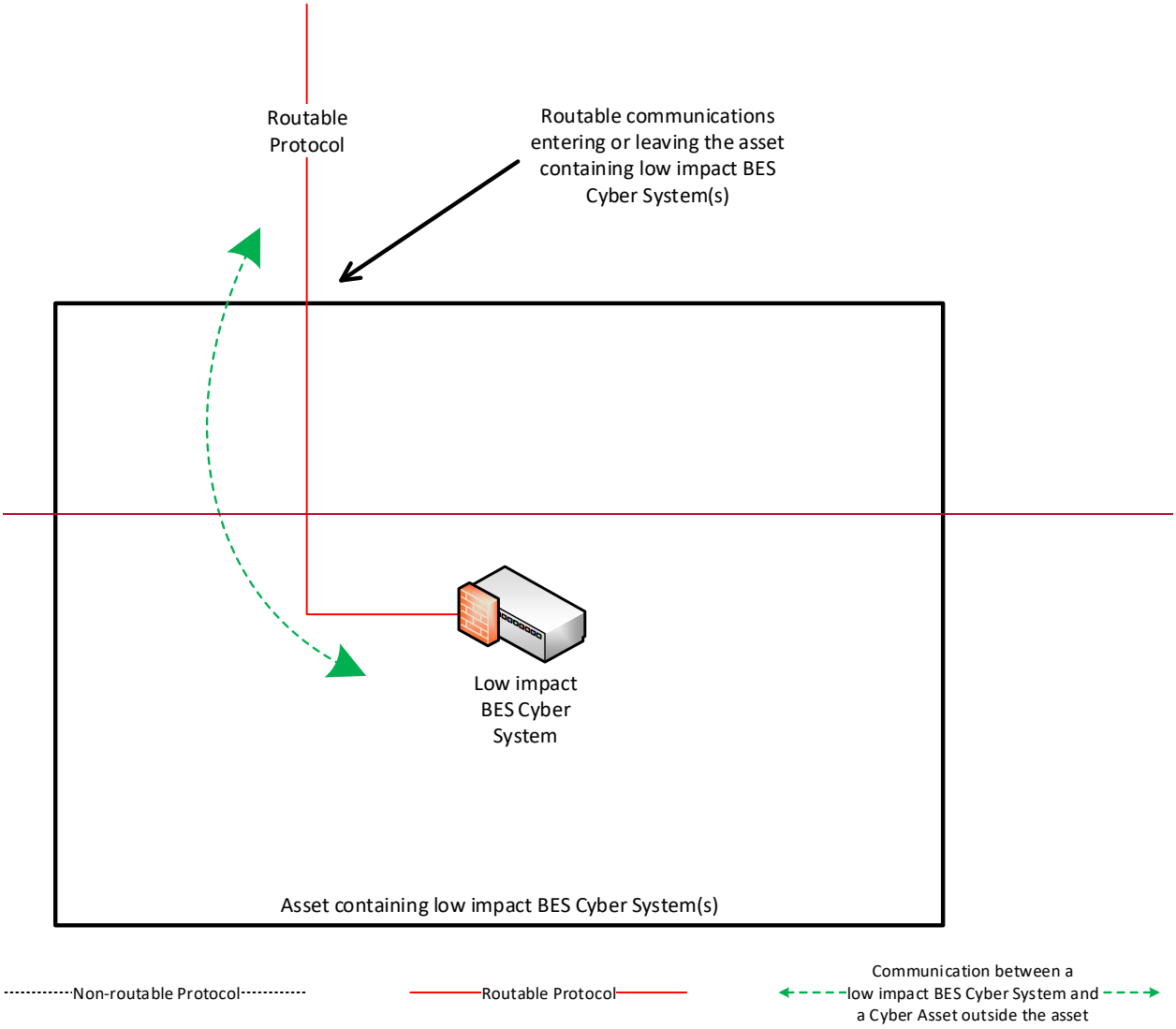
~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

~~NOTE:~~

- ~~This is not an exhaustive list of applicable concepts.~~
- ~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

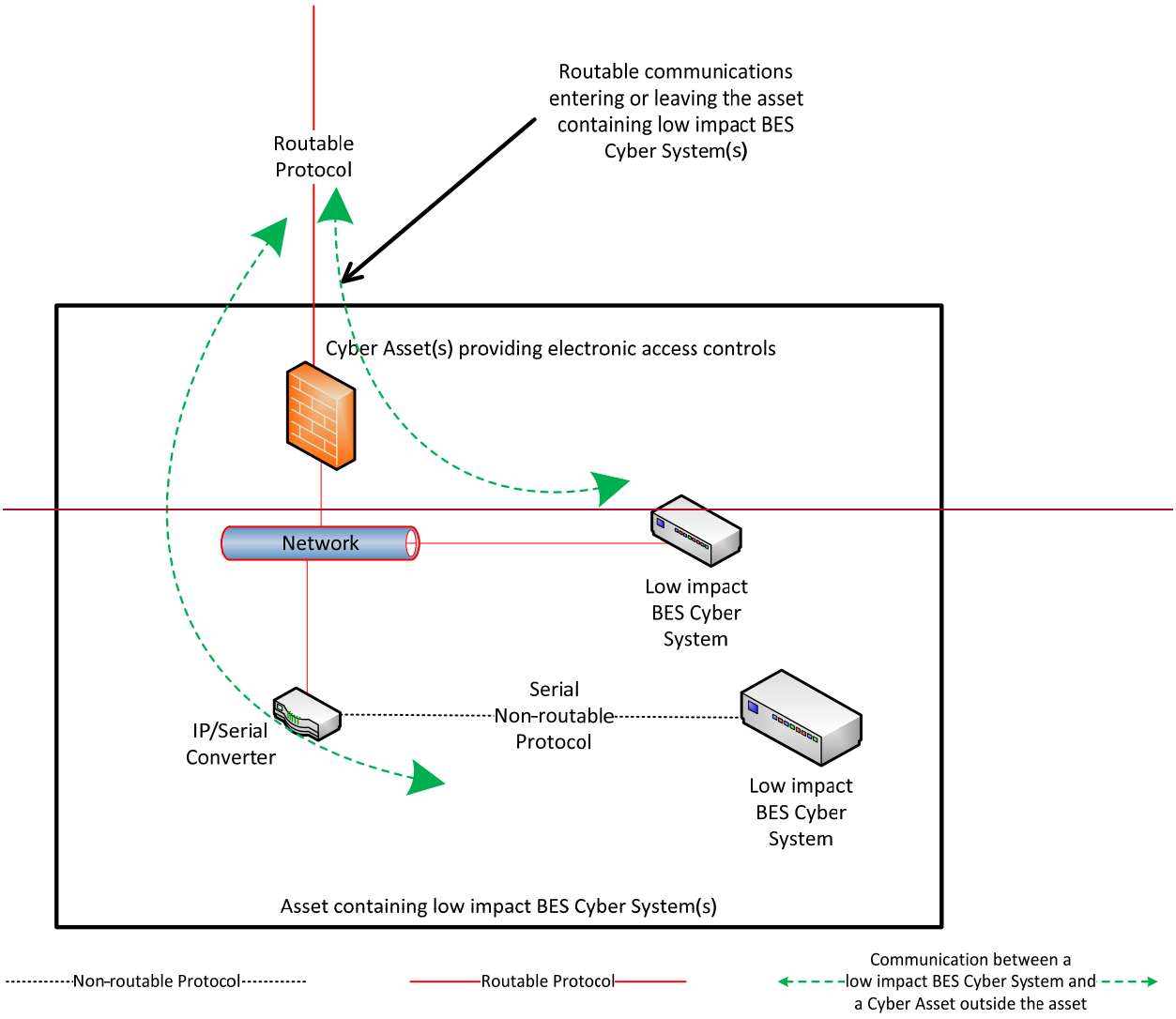
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 1*~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

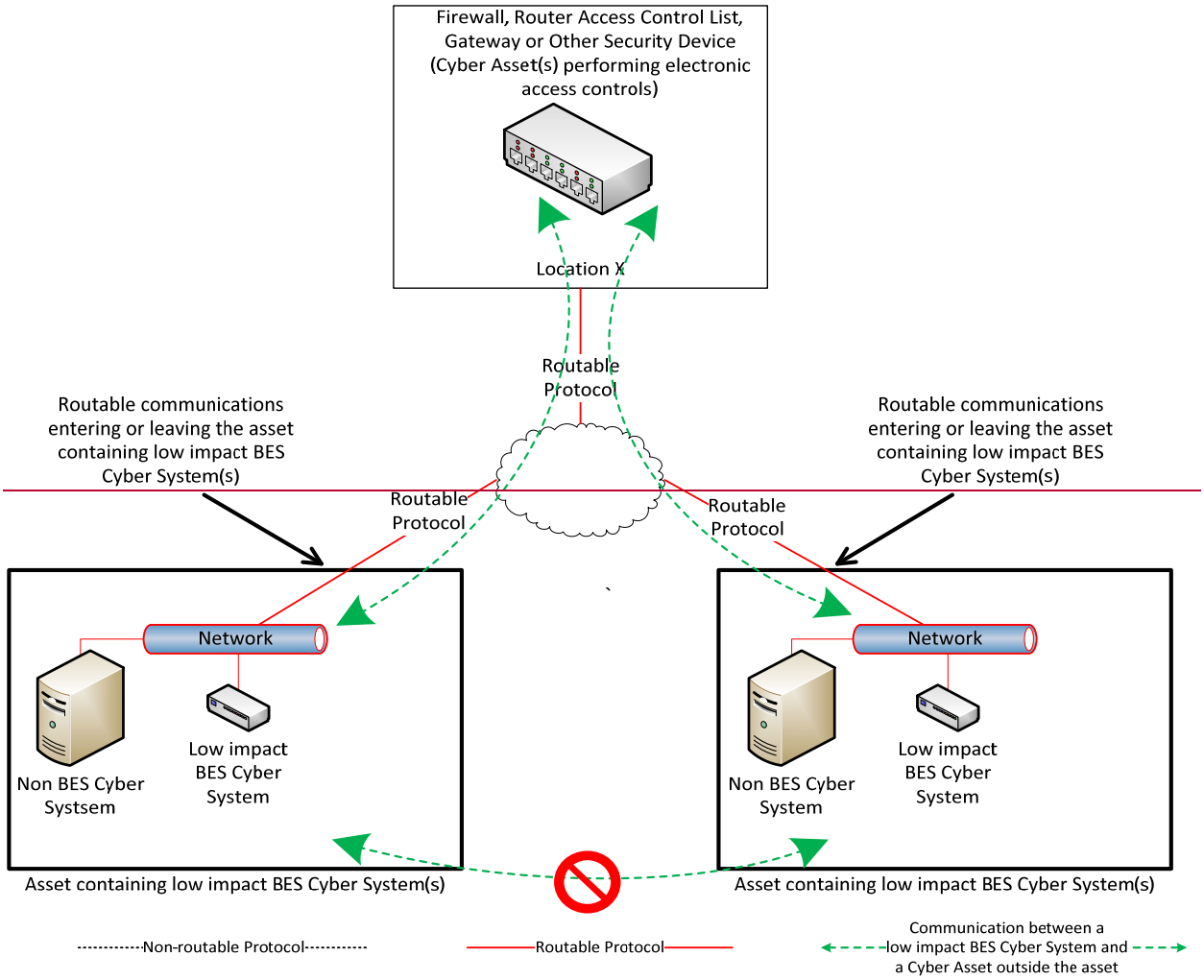
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 2*~~

~~Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

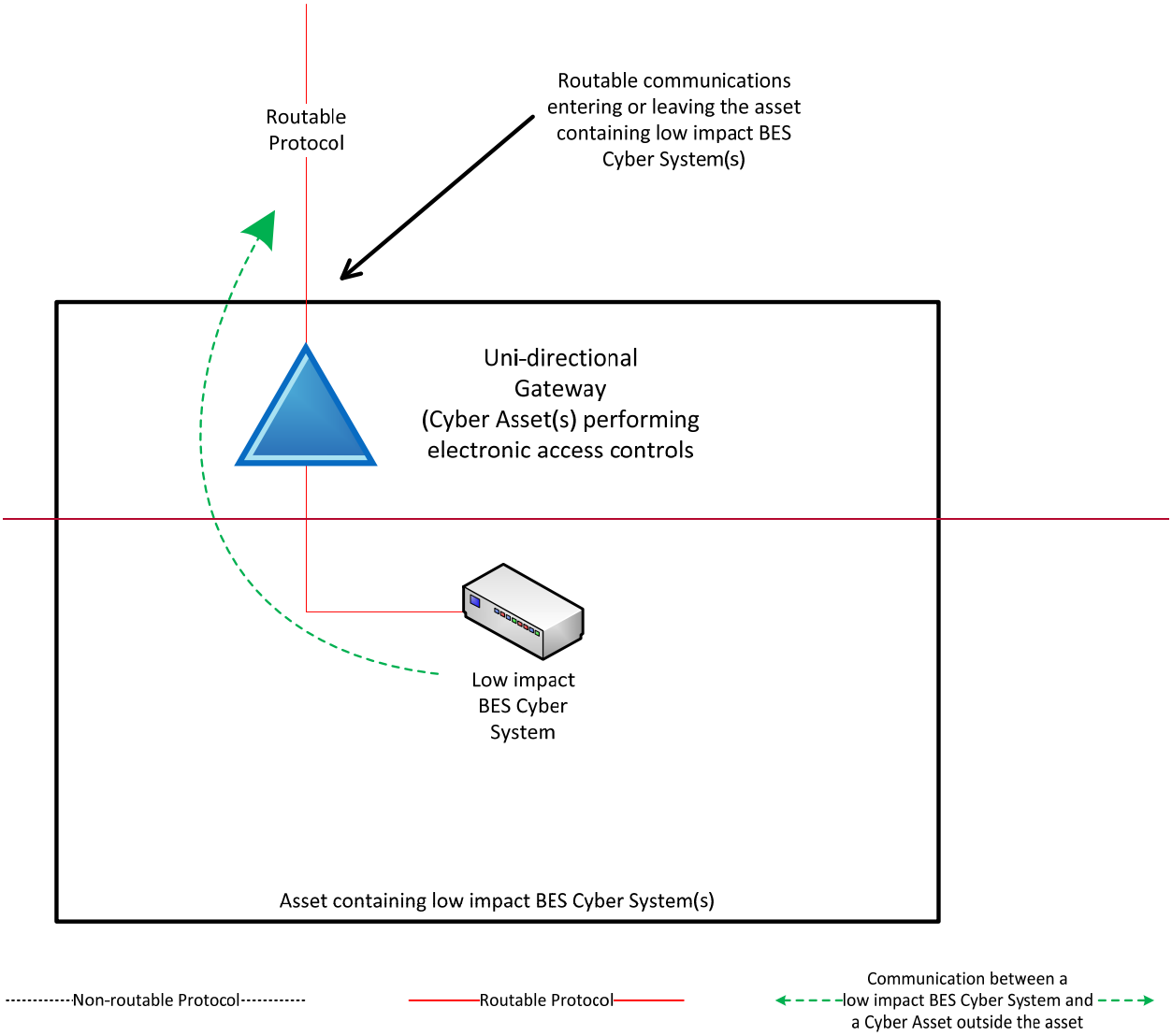
~~The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 3*~~

~~Reference Model 4 – Uni-directional Gateway~~

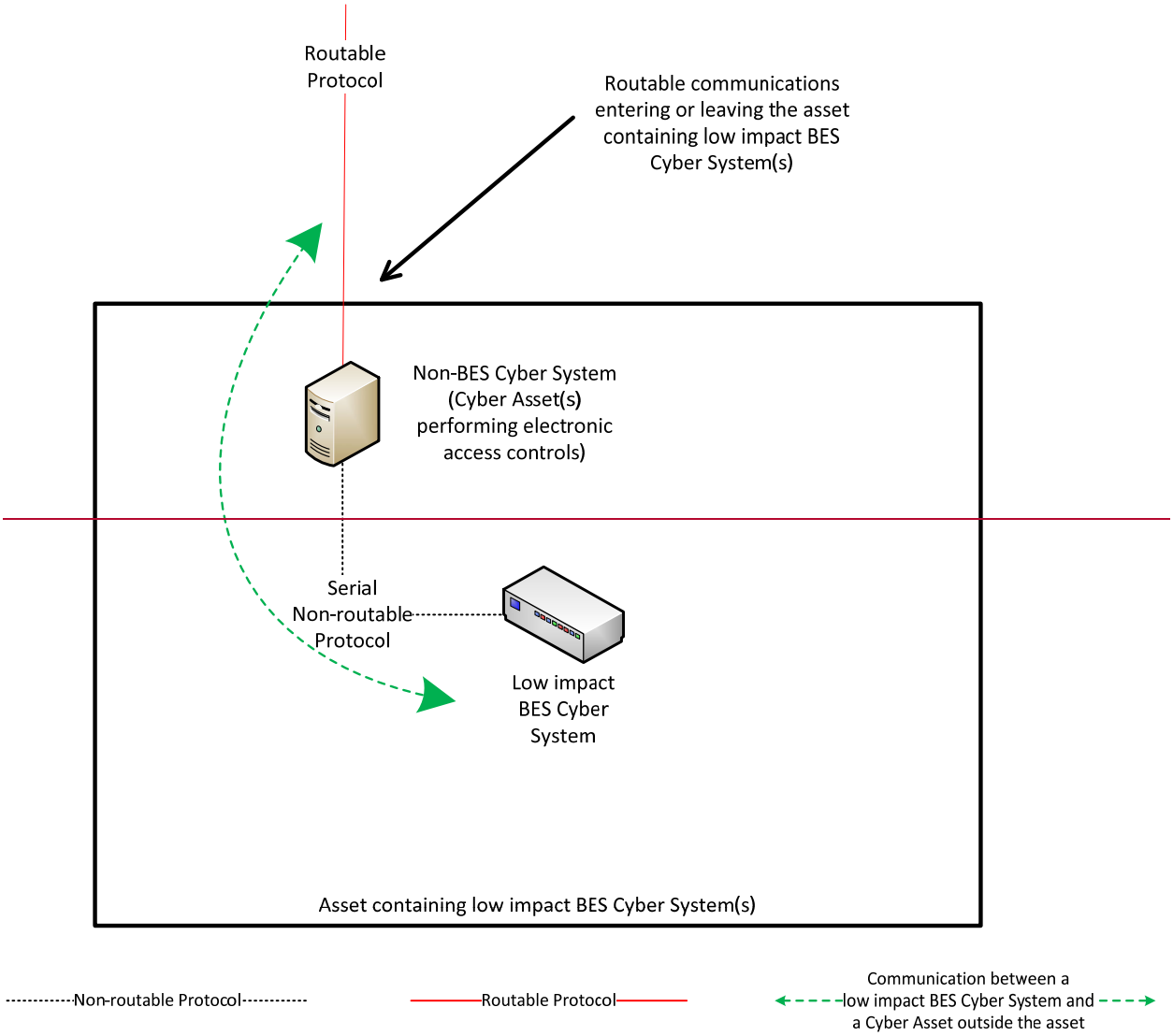
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~



~~*Reference Model 4*~~

~~Reference Model 5 – User Authentication~~

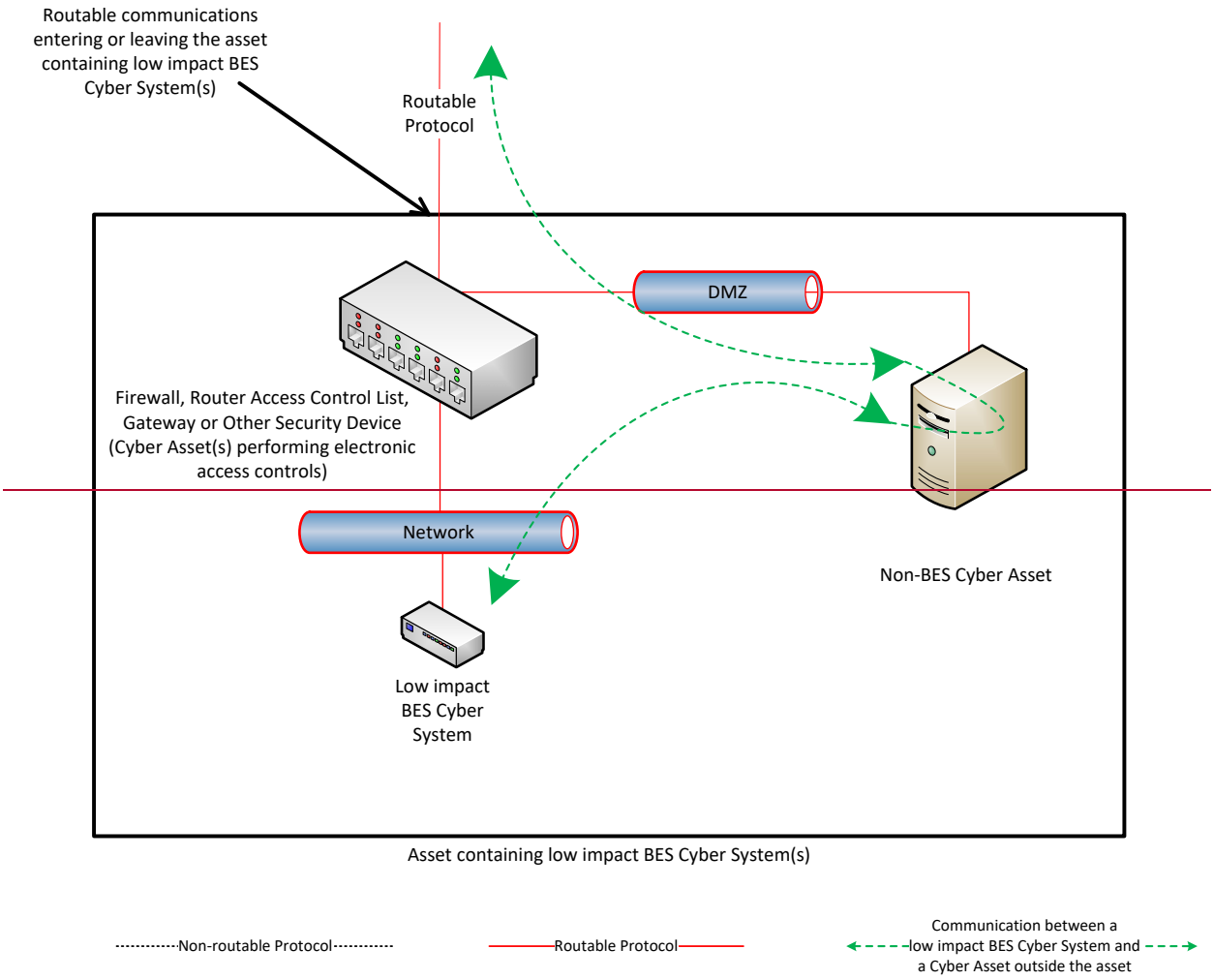
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~



~~Reference Model 5~~

~~Reference Model~~ 6 ~~– Indirect Access~~

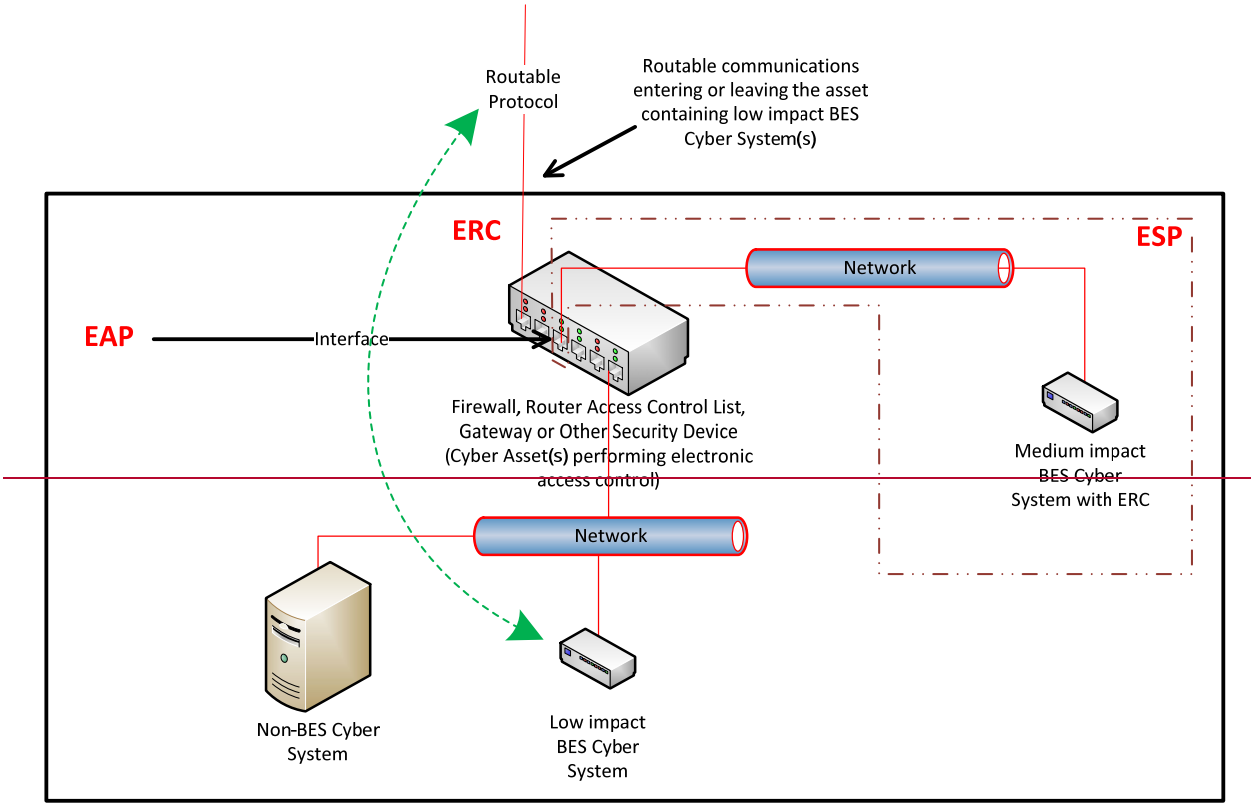
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~



~~*Reference Model 6*~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~Reference Model 7~~

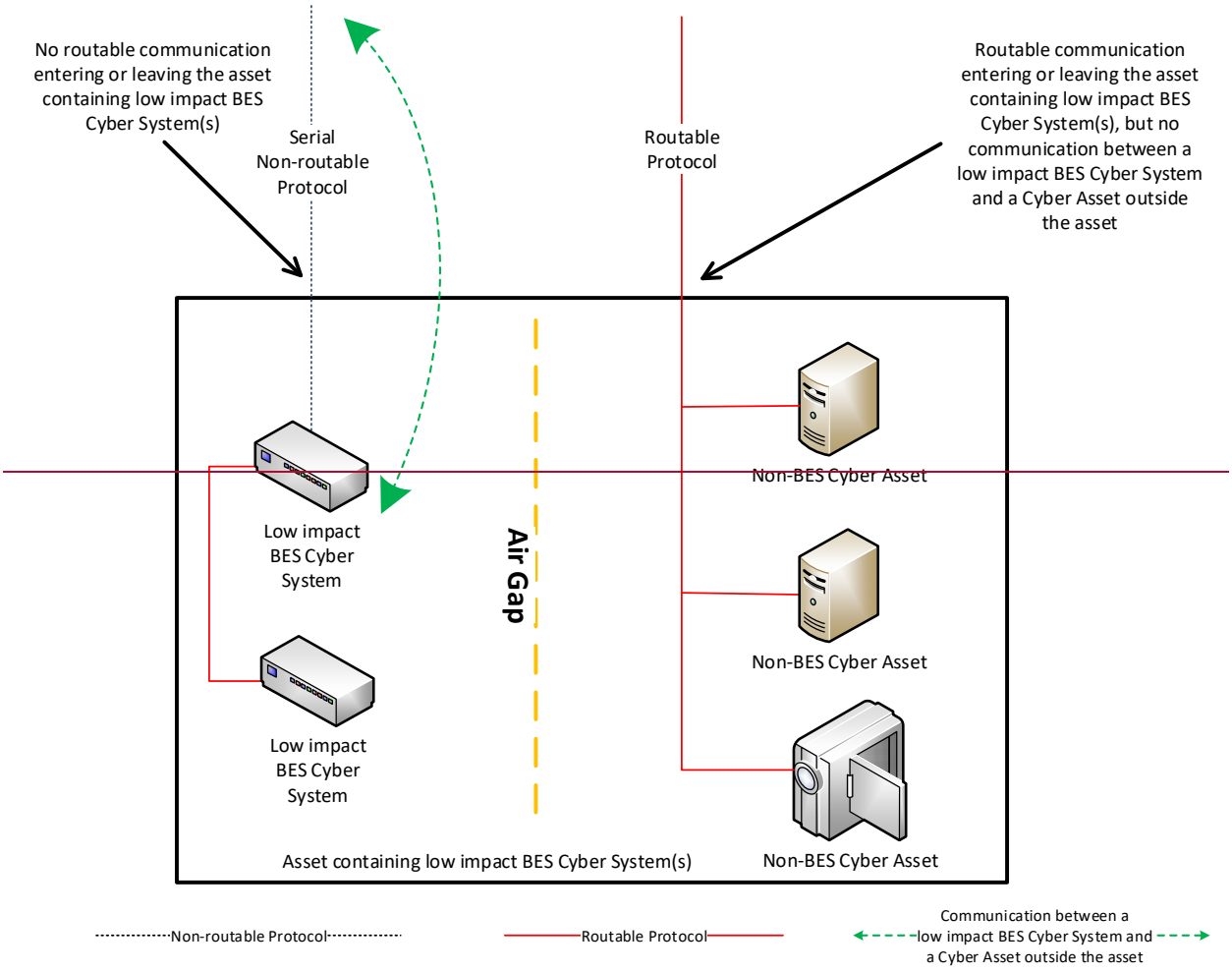
Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

0) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;

0) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.

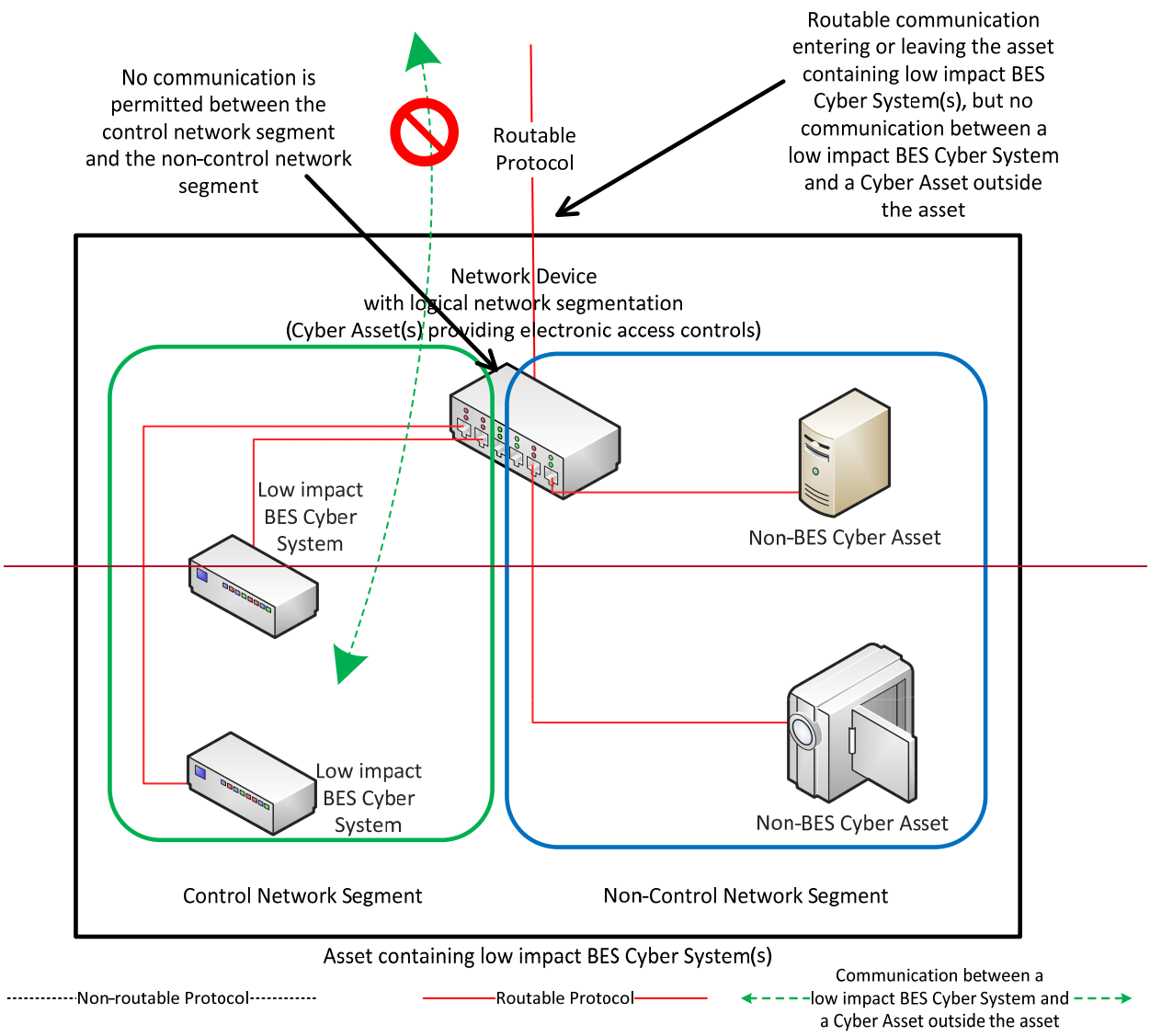
0) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).



~~*Reference Model 8*~~

~~Reference Model 9 – Logical Isolation – No Electronic Access Controls Required~~

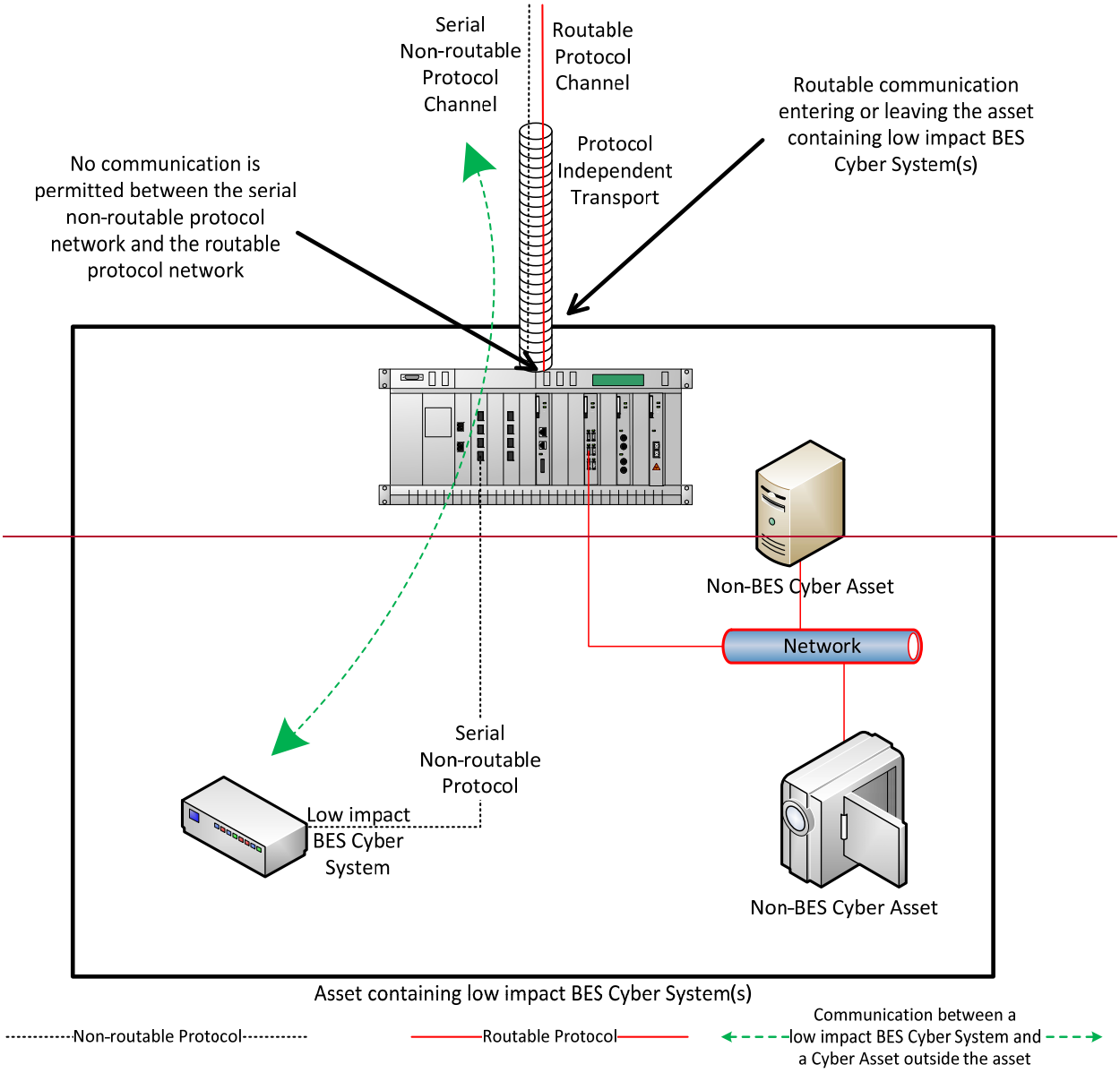
~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~



~~*Reference Model 9*~~

~~**Reference Model 10 – Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required**~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~*Reference Model 10*~~

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

~~Malicious Code Risk Mitigation~~

~~The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~Section 5.1:~~ ~~Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[‡] Procurement language may unify

[‡] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System

~~network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.~~

~~Requirement R3:~~

~~The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.~~

~~Requirement R4:~~

~~118.~~4. ~~As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous~~ .1, documentation ~~records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.~~showing:

~~The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is~~

~~named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

~~and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~Rationale for Section 5 of Attachment 1 (Requirement R2):~~
~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~
~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-9 — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below.

Reliability Standard CIP-003-9

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-9 shall become effective on the first day of the first calendar quarter that is 36 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

[1] See Applicability section of CIP-003-9 for additional information on Distribution Providers subject to the standard.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-9 shall become effective on the first day of the first calendar quarter that is 36 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-9 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-9.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-9 within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-9 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit C

Order No. 672 Criteria

EXHBIIT D

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standard has met or exceeded the criteria.

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]

The proposed Reliability Standard CIP-003-9 would advance the reliability of the Bulk-Power System ("BPS") through enhanced supply chain risk management for low impact BES Cyber Systems. Proposed Reliability Standard CIP-003-9 includes requirements for Responsible Entities to implement vendor electronic remote access security controls including detecting and disabling such access and detecting malicious communications over such access.

As discussed more fully in the main section of NERC's petition, NERC developed the proposed standard to address recommendations from the NERC Staff Reports (**Exhibit E**) that

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006) [hereinafter Order No. 672].

[2] *See* Order No. 672, *supra* note 1, at P 321 ("The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cybersecurity protection.").

See Order No. 672, *supra* note 1, at P 324 ("The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.").

assessed supply chain risks for low impact BES Cyber Systems. One of the most significant risks identified was vendor employee remote access to BES Cyber Systems, and the proposed Reliability Standard requires controls around such access, as recommended by the NERC Staff Reports (**Exhibit E**). The proposed Reliability Standard is designed to achieve a specific reliability goal (mitigation of supply chain risk), and contains a technically sound means to achieve that goal.

2. Proposed Reliability Standards must be applicable only to users, owners, and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. Proposed Reliability Standard CIP-003-9 would apply to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standard clearly articulates the actions that applicable entities must take to comply with the standards.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment, as discussed further in **Exhibit D**. The assignment of the severity level for each VSL is consistent with the corresponding requirement, and the VSLs should ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology,

---

[3] *See* Order No. 672, *supra* note 1, at P 322 ("The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.").

See Order No. 672, *supra* note 1, at P 325 ("The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.").

[4] *See* Order No. 672, *supra* note 1, at P 326 ("The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.").

thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criteria or measures for compliance, so that it can be enforced in a consistent and non-preferential manner.[5]

The proposed Reliability Standard contains measures that support each requirement by clearly identifying what is required and how the requirement will be enforced. These measures help provide clarity regarding how the requirements would be enforced and help ensure that the requirements would be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

5. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently, but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]

The proposed Reliability Standard achieves its reliability goals effectively and efficiently in accordance with Order No. 672. Proposed Reliability Standard CIP-003-9 would achieve the reliability goal of mitigating supply chain risks for low impact BES Cyber Systems through requirements tailored to the impact of those systems.

6. Proposed Reliability Standards cannot be "lowest common denominator," i.e., cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]

---

[5] *See* Order No. 672, *supra* note 1, at P 327 ("There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

[6] *See* Order No. 672, *supra* note 1, at P 328 ("The proposed Reliability Standard does not necessarily have to reflect the optimal method, or 'best practice,' for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.").

[7] *See* Order No. 672, *supra* note 1, at P 329 ("The proposed Reliability Standard must not simply reflect a compromise in the ERO's Reliability Standard development process based on the least effective North American practice—the so-called 'lowest common denominator'—if such practice does not adequately protect Bulk-Power

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. The proposed Reliability Standard would enhance reliability by mitigating supply chain risk to low impact BES Cyber Systems through controls consistent with the recommendations of the NERC Staff Reports (**Exhibit E**).

7. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]

The proposed Reliability Standard would apply consistently throughout North America and would not favor one geographic area or regional model. The proposed Reliability Standard would provide sufficient flexibility to accommodate regional/geographic variations, including climate, generation type, market issues, state rules, and other considerations.

System reliability. Although the Commission will give due weight to the technical expertise of the ERO, we will not hesitate to remand a proposed Reliability Standard if we are convinced it is not adequate to protect reliability.").

See Order No. 672, *supra* note 1, at P 330 ("A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a 'lowest common denominator' Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.").

[8] *See* Order No. 672, *supra* note 1, at P 331 ("A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System, to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.").

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standard would have no undue negative effect on competition and would not unreasonably restrict the available transmission capacity or limit the use of the BPS in a preferential manner. The proposed Reliability Standard would require the same performance by each of the applicable entities.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed effective date for the proposed Reliability Standard is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop necessary procedures or other relevant capability. The proposed implementation plan provides that the proposed Reliability Standard would become effective on the first day of the first calendar quarter that is thirty-six (36) months after applicable regulatory approval. The proposed implementation plan reflects consideration that there are a large number of low impact BES Cyber Systems and Responsible Entities need time to procure and install equipment that may be subject to delays given high demand. The proposed implementation plan is attached as **Exhibit B** to this petition.

---

[9] *See* Order No. 672, *supra* note 1, at P 332 ("As directed by section 215 of the FPA, the Commission itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.").

[10] *See* Order No. 672, *supra* note 1, at P 333 ("In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved, ANSI-accredited processes for developing and approving Reliability Standards. **Exhibit G** includes a summary of the Reliability Standard development proceedings, and details the processes followed to develop the proposed Reliability Standard. These processes included, among other things, comment periods, pre-ballot review periods, and balloting periods. Additionally, all meetings of the standard drafting team were properly noticed and open to the public.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standard. No comments were received that indicated that the proposed Reliability Standard conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.

---

[11] *See* Order No. 672, *supra* note 1, at P 334 ("Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by the Commission.").

[12] *See* Order No. 672, *supra* note 1, at P 335 ("Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.").

[13] *See* Order No. 672, *supra* note 1, at P 323 ("In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.").

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2020-03 Supply Chain Low Impact Revisions

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-003-9. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-003-9, Requirement R1

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR	did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR	did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was modified by adding a seventh topic to Requirement R1.2 for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to review one or more documented cyber security policies covering the topics specified in Requirement R1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-9, Requirement R2

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement	according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic	authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	

VSL Justifications for CIP-003-9 Requirements R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was not modified but the attachment referenced in the requirement was. The attachment was modified by adding a sixth section for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented cyber security plans covering the sections specified in Attachment 1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-003-9 Requirements R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-9, Requirement R3
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-9, Requirement R3
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VRF Justification for CIP-003-9, Requirement R4
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-9, Requirement R4
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E

NERC Staff Reports

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-1

Cyber Security Supply Chain Risks

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Supply Chain Risks

Staff Report and Recommended Actions

May 17, 2019

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

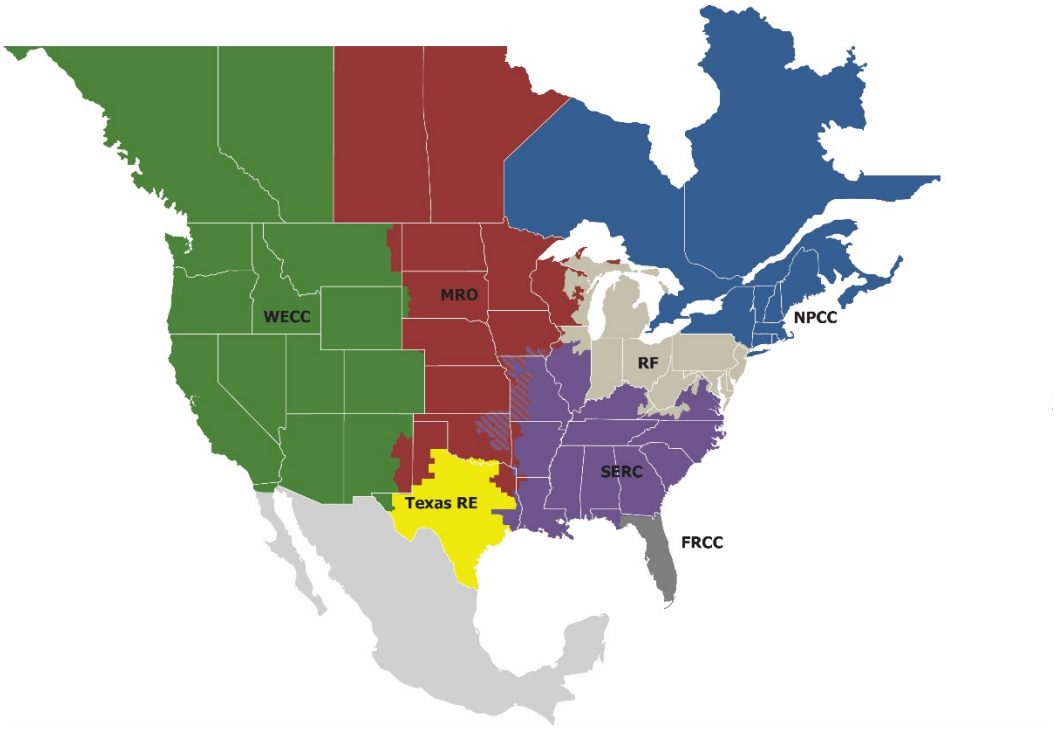
Acknowledgements

Apart from the efforts of NERC staff, the success of any report depends largely on the guidance and input of many others. NERC wishes to take this opportunity to express a special thanks to Dr. Joseph Baugh of the Western Electricity Coordinating Council and Ray Sefchik of Reliability First for their exceptional contributions in helping to improve the content of this report. NERC also wishes to take this opportunity to express a special thanks to the Critical Infrastructure Protection Committee Supply Chain Working Group for their valuable contribution to this report. The authors also acknowledge and appreciate the significant contributions from individuals, working groups, subject matter experts, and organizations whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this report.

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

The supply chains for information and communications technology and industrial control systems may provide various opportunities for adversaries to initiate cyber attacks, thereby presenting risks to Bulk Electric System (BES)[1] security. NERC is committed to using its many reliability tools to support industry's efforts to mitigate supply chain risks.

In 2017, NERC developed new and revised critical infrastructure protection (CIP) Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards will be applicable to the highest-risk systems that have the greatest impact to the grid. The Supply Chain Standards will require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure responsible entities manage supply chain risks to those systems through the procurement process, thereby reducing the risk that supply chain compromise will negatively impact the BPS.

When adopting the Supply Chain Standards in August 2017, the NERC Board of Trustees (Board) directed NERC to undertake further action on supply chain issues. Among other things, the NERC Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards and develop recommendations for follow-up actions that will best address identified risks.

In this report, NERC documents the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommends actions to address those risks.

Upon evaluation of the potential supply chain risks presented by Electronic Access Control or Monitoring Systems (EACMSs), and in response to the directive of FERC in Order No. 850 to include such systems within the scope of the Supply Chain Standards,[2] NERC staff recommends revising the Supply Chain Standards to address EACMSs that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.

Additionally, based on the supply chain risks presented by such assets, NERC staff recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACSs) that provide physical access control (excluding alarming and logging) to high- and medium-impact BES Cyber Systems.

At this time and based on the available information, NERC staff does not recommend modification of the Supply Chain Standards to include all low impact BES Cyber Systems. NERC staff recommends further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity as follows: first, by issuing a Request for Data or Information pursuant to Section 1600 of the NERC Rules of Procedure; and second, by continued monitoring of the application of the criteria in CIP Reliability Standards that differentiate medium impact BES Cyber Systems from low impact through the use of industry surveys and questionnaires following the implementation of the Supply Chain Standards. To address the potential risks associated with the supply chain for such systems prior to completion of this study, NERC staff will work with the Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

[1] Unless otherwise indicated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[2] Order No. 850, *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020, at P 30 (2018) ("Order No. 850").

Due to varying levels of risk, NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities with evaluating their Protected Cyber Assets (PCAs) on a case-by-case basis to determine what, if any, additional supply chain protections are needed.

NERC staff recommends that entities refer to industry practices and guidelines, such as those developed by the North American Transmission Forum, the American Public Power Association and National Rural Electric Cooperative Association, and the North American Generator Forum, when developing their CIP-013-1 process(es) for the procurement of BES Cyber Systems.

Because supply chain risks are complex and constantly evolving, NERC staff also recommends conducting additional data collection on BES supply chain risk management through the use of industry surveys and questionnaires. Such evaluation may result in additional recommendations for future actions. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.

Next Steps on Recommendations

NERC will work through its existing processes with stakeholders to review NERC staff's recommendations and determine appropriate follow up actions.

Introduction

Background

In recent years, the Federal Energy Regulatory Commission (FERC or the Commission), NERC, and the industry have identified risks from the supply chain as a potential threat to BES reliability. Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in a multitude of countries across the globe. In procuring products and services for their operations, BPS owners and operators typically rely on vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. Malicious actors may target one or more vendors in the supply chain to create or exploit vulnerabilities that could then be used to initiate cyber attacks on BES Cyber Systems and equipment.

On July 21, 2016, FERC issued Order No. 829,[3] directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as follows:

> "[FERC directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[4]

Following the issuance of Order No. 829, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3.

The Supply Chain Standards support reliability by requiring responsible entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact BES Cyber Systems. Consistent with Order No. 829, the proposed Reliability Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Reliability Standard CIP-013-1 requires responsible entities to develop and implement plans to address supply chain cyber security risks during the planning and procurement of high and medium impact BES Cyber Systems. Modifications in CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.

The Board adopted the Supply Chain Standards at its August 10, 2017, meeting. FERC approved the Supply Chain Standards with directives for additional modifications to address EACMSs in Order No. 850, issued October 18, 2018.[5]

[3] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards,* 156 FERC ¶ 61,050 (2016).
[4] *Id.* at P 2 (internal citation omitted); *see also id*. at PP 44-45.
[5] Order No. 850, *supra* note 1.

August 2017 Board Resolutions

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to implementation and risk evaluation.[6] The resolutions outline six actions for NERC management and stakeholders to take in assisting with the implementation and evaluation of the Supply Chain Standards as well as other actions to address potential supply chain risks for assets not currently subject to the standards.

The Board's August 2017 resolutions include the following:

- **Support Effective and Efficient Implementation of the Supply Chain Standards:** The Board requested that NERC promptly commence preparations for the implementation of the Supply Chain Standards by using similar methods during the transition to version 5 of the CIP Reliability Standards and report regularly to the Board on those activities.
- **Cyber Security Supply Chain Risk Study:** The Board requested that NERC, in collaboration with others, study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks. The Board requested that NERC submit an interim report within 12 months and a final report within 18 months. NERC presented the interim report to the Board in August 2018.
- **Communicate Supply Chain Risks to Industry:** The Board requested that NERC communicate supply chain risk developments and risks to industry in connection with the Cyber Security Supply Chain Risk Study (i.e. this report).
- **Forum White Papers:** The Board requested that the North American Transmission Forum (NATF) and the North American Generation Forum (NAGF) (collectively, the "Forums") develop (and distribute as permissible) white papers to address best and leading practices in supply chain management as described in the resolution.
- **Association White Papers:** The Board requested that the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) (collectively, the "Associations") develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, as described in the resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.
- **Evaluate Supply Chain Standard Effectiveness:** The Board requested that NERC, in collaboration with technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards as described in the resolution and report to the Board.

The activities undertaken by NERC, the Forums, and the Associations to address the Board's supply chain resolutions are designed to establish a collective understanding of the supply chain risk to the BES and activities to mitigate those risks.

This report addresses the Board's second resolution, which is to prepare a study of cyber security supply chain risks. Building upon the interim report presented to the Board in August 2018 (discussed below), this report addresses the risks associated with low impact BES Cyber Systems, EACMSs, PCAs, and PACSs and the actions that should be taken to address those risks. This report also makes reference to certain white papers and guidance documents prepared by the Forums and Associations in response to the Board's fourth and fifth directives.

[6] The Additional Resolutions for Agenda Item 9.a: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1, NERC Board of Trustees Meeting, August 10, 2017, is available at the following: http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

All reports are posted on NERC's website under the Supply Chain Risk Mitigation Program Initiative[7] page. In Appendix A to this report, NERC summarizes the activities taken to address the other Board resolutions.

EPRI Interim Report (August 2018)

NERC engaged the Electric Power Research Institute (EPRI) to provide an independent assessment of industry supply chain risks to facilitate NERC's supply chain risk study. NERC presented EPRI's report, titled *EPRI Supply Chain Risk Assessment Report*,[8] to the Board in August 2018. In this report, EPRI contributed the following actions:

- Performed an assessment of product/manufacturer types used on the BES for Supervisory Control and Data Acquisition (SCADA), network and telecommunications, and commercial off the shelf operating systems
- Provided an analysis of emerging best practices and standards used in other industries to mitigate supply chain risks, concentrating on practices currently not considered in the scope of the existing CIP Reliability Standards
- Provided a study of the applicability of the CIP Reliability Standards to supply chain risks
- Provided a list of recommendations to reduce residual supply chain risks and facilitate the collection of additional information for future evaluation, so that, prior to any changes in policy, data can be obtained, assessed, and discussed in a transparent manner

Forum and Association White Papers

In response to the Board's fourth resolution, the NATF and NAGF each prepared White Papers that provide considerations for their member entities on implementing robust cyber security risk management plans and programs.

The NATF White Paper, titled *Cyber Security Supply Chain Risk Management Guidance*,[9] recommends several best and leading practices for members in establishing and implementing their supply chain risk management programs. These practices include considerations for procurement, specification, vendor requirements, and managing existing equipment activities. NATF's White Paper identifies three hallmarks of an effective program, including foundational practices that coordinate supply chain and cyber security risk management efforts; organization-wide communication where supply chain risk management is supported throughout the business and implemented throughout the system-development life cycle; and risk management processes with clearly defined criteria, risk evaluation, and risk response components.

The NAGF White Paper, titled *Cyber Security Supply Chain Management*,[10] identifies examples for generation entities to consider when developing and implementing their cyber security risk management plans. The NAGF White Paper describes a risk-based approach by which entities conduct an initial screen to determine where additional vendor supply chain risk assessments are required, taking into account the entity's cyber assets impact rating criteria, asset connectivity, vendor connectivity, presence of Transient Cyber Assets and Removable Media, support staff considerations, security awareness/training considerations, and considerations related to Personnel Risk

[7] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx
[8] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").
[9] NATF, *Cyber Security Supply Chain Risk Management Guidance* (June 20, 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf ("NATF White Paper").
[10] NAGF, *Cyber Security Supply Chain Management White Paper* (2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF%20SC%20White%20Paper%20final.pdf ("NAGF White Paper").

Assessments performed for staff and contractors. If the entity determines that a risk assessment is required, the entity should consider the level of risk posed by the vendor itself and the product or service it provides to determine the appropriate level of supply chain controls required. The NAGF White Paper describes several vendor risk attributes and product/service attributes for the entity to consider in evaluating potential risks.

In response to the Board's fifth resolution, APPA and NRECA prepared a White Paper, titled *Managing Cyber Supply Chain Risk – Best Practices for Small Entities*.[11] The APPA/NRECA White Paper identified several practices for smaller entities with low impact BES Cyber Systems to consider in managing risks from the supply chain. APPA and NRECA identified several best practices for its member entities to consider based on interviews with several smaller entities regarding their supply chain risk management programs. These best practices include, among other things:

- Organizational aspects, such as having senior leadership support for supply chain risk management and conducting enterprise-wide cyber risk assessments;
- Selecting vendors with an eye toward reducing supply chain risk, including using well-known, trusted, and established vendors and considering vendors who have completed third-party accreditation or self-certification of their supply chain practices;
- Placing appropriate limitations surrounding vendor remote access to systems; taking steps to ensure software integrity prior to installation;
- Placing appropriate controls around software updates and patch management.

Order No. 850 Approving the Supply Chain Standards

FERC approved the Supply Chain Standards in Order No. 850, issued on October 18, 2018. While finding that the standards addressed the Commission's directive in Order No. 829 and constitute "substantial progress" in addressing supply chain cyber security risks, the Commission also issued two directives to NERC.

First, noting the significant role that EACMSs play in the protection scheme for medium and high impact BES Cyber Systems, the Commission found that excluding EACMSs from the scope of the Supply Chain Standards presents risks to the cyber security of the BES. Therefore, the Commission directed NERC to develop modifications to the standards to address EACMSs associated with medium and high impact BES Cyber Systems and to submit those modifications within 24 months of the effective date of the final rule.[12]

Second, while continuing to express its concern that excluding certain categories of assets (PACSs and PCAs) from the standards could pose a reliability risk, the Commission found that NERC is taking "adequate and timely steps" to study whether these items should be included in the standards. The Commission accepted NERC's commitment to evaluate the risks of PACSs and PCAs (in addition to low impact BES Cyber Systems) in its study of cyber security supply chain risks and directed NERC to file the final report with FERC upon its completion. The Commission stated that it would be in a better position to consider what further steps, if any, should be taken to protect reliability after receipt of this final report.[13]

Under the approved implementation plan, the Supply Chain Standards will become effective in the United States on the first day of the first calendar quarter that is 18 months after the effective date of the final rule, which is July 1, 2020.

[11] APPA/NRECA, *Managing Cyber Supply Chain Risk – Best Practices for Small Entities* (Apr. 25, 2018), https://www.cooperative.com/programs-services/government-relations/regulatory-issues/documents/supply%20chain%20white%20paper%204-25%20final.pdf ("APPA/NRECA White Paper").
[12] Order No. 850 at P 30.
[13] Order No. 850 at PP 31, 67.

Chapter 1: Supply Chain Risks to the Bulk Electric System and Standards and Practices for Addressing those Risks

Overview

In recognition of the potential risks to BES reliability posed by supply chain vulnerabilities, NERC developed the Supply Chain Standards. These standards will require responsible entities to take additional actions to address cyber security risks associated with the supply chain for BES Cyber Systems.

Consistent with the risk-based approach of the CIP Reliability Standards, and as discussed more fully below, the Supply Chain Standards are applicable only to certain categories of assets. As discussed in subsequent sections of this report, revisions to the Supply Chain Standards may be necessary to help ensure that the standards adequately address supply chain risks related to certain assets that are not within the current scope of the standards.

In addition to the Supply Chain Standards, industry may use other standards and best practices to mitigate potential supply chain risks. Understanding these standards and best practices helps to create a fuller understanding of supply chain risks and the steps that may be taken to help address them in the context of BES reliability.

Supply Chain Risks

Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in countries across the globe. Multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single purchased product. Global supply chains can provide the opportunity for substantial benefits to consumers, but at the same time, a vulnerability at any link in the chain could result in risks to the end user.

These risks, like the supply chains themselves, are global, multidimensional, and constantly evolving. As observed by FERC, cyber supply chain risks may stem from insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development processes.[14] Even well-designed products may have malicious components introduced in the supply chain, and it may prove difficult to identify these components before they are deployed.

Over time, NERC and the industry have developed a more sophisticated understanding of the potential impacts these supply chain risks could have on BES reliability:

- In its 2018 Guidance, the NATF highlighted several real-world events that help demonstrate the risk supply chain vulnerabilities could pose to the electric power industry. These events included the installation of malicious software and theft of project files on a SCADA offering, insertion of unauthorized code on a firewall solution that allowed for the execution of remote procedures, and the alleged insertion of a foreign entity "backdoor" into an anti-virus company's security products.[15]
- In its 2018 White Paper, the APPA and NRECA identified the risks posed by the introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems as two of the most significant supply chain risks facing their member entities.[16]

[14] *Revised Critical Infrastructure Protection Reliability Standards*, 152 FERC ¶ 61,054, at P 62 (2015).
[15] NATF White Paper at 6.
[16] APPA/NRECA White Paper at 2.

- The *EPRI Interim Report*[17] further highlighted that a compromise in a single vendor's supply chain could have widespread impacts where the vendor supplies a substantial portion of a given product market.[18]

A number of standards and best practices have been developed to address supply chain risks in the electric power industry and other industries. These standards and best practices provide a more complete understanding of supply chain risks and the steps entities may take to mitigate them. Additionally, the Supply Chain Standards provide strong protections for certain categories of high-risk BES Cyber Assets. In implementing the Supply Chain Standards, responsible entities should incorporate some of these industry standards and best practices into their Reliability Standard CIP-013 Requirement R1 supply chain risk management plan(s). NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in selecting which standards and best practices are appropriate.

The Supply Chain Standards, however, do not mandate that entities provide protections for all categories of potentially vulnerable assets. Different categories of assets would present different risks if compromise based on the type of asset and its function. In subsequent sections, this report provides further information on these devices, provides recommendations for the steps entities should take to reduce their exposure to such risks, and, where appropriate, recommends further changes to the Supply Chain Standards to address the risks associated with these specific devices.

Industry Standards and Best Practices to Address Supply Chain Risks

Supply chain concerns are not unique to the electric power industry. Other industries that are sensitive to such risks have developed standards and best practices to mitigate supply chain risks. These standards and best practices, which are discussed in Chapter 3 of the EPRI Interim Report, may provide considerations for mitigating supply chain risks in the electric power industry context as well.

Relevant standards and best practices include the following:

- **Off-premise Supplier Services:** In the government context, where a supplier performs deployments or services for an entity involving federal information systems that are not on government premises, the Federal Risk and Authorization Management Program (FedRAMP) standards apply.
- **Third-Party Accreditation Processes:** Suppliers that follow standards, such as FedRAMP and quality management and information security management standards published by the International Organization for Standardization, use independent third parties to assess their adherence to the standards.
- **Secure Hardware Delivery:** The Energy Sector Control Systems Working Group of the U.S. Department of Energy (DOE) developed Cybersecurity Procurement Language for Energy Delivery Systems that identified controls for hardware delivery to help reduce the risk of compromise during transport.
- **Provenance:** Provenance is the ability to provide traceability in the supply chain processes and supplier relationships. Several standards and guidelines address provenance, including the National Supply Chain Risk Management Practices for Federal Information Systems (NISTIR 7622) published by the National Institute of Standards and Technology (NIST).

[17] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").

[18] *See generally* EPRI Interim Report at Chapter 2.

- **Threat Modeling:** Threat modeling is a process employed to ensure that all products have a threat model specific to the current development scope of the product as described in International Electrotechnical Commission standard IEC 62443-4-1.
- **Supply Chain Deficiencies Assessment:** Addressing the controls for identifying and mitigating the risk of assessed vulnerabilities or inherent weaknesses in the supply chain process of certain product or service providers is an important risk management approach as described in NIST SP 800-53. The NATF white paper highlights how such an approach may apply to supply chain risk management for BES cyber systems.[19]
- **External Dependencies Recognition:** One aspect considered by the DOE's Cyber Security Capabilities Maturity Model (C2M2) is considering supply chain as a process of identifying and managing external dependencies. Recognizing dependencies and those that are most critical to operations can improve an entity's ability to highlight and mitigate supply chain risks.
- **Policy for Handling Supplied Products or Services that Do Not Adhere to Procurement Processes:** Entities may use controls to mitigate risks when products or services are supplied that do not adhere to their specific supply chain policies. Such an approach is described by the U.S. Nuclear Regulatory Commission in Appendix B to 10 C.F.R. part 50 in the context of quality assurance. Attachment A of the *NATF Cyber Security Supply Chain Risk Management Guidance* document provides examples of controls used when procuring BES Cyber Assets and services.[20]
- **Unsupported or Open-Sourced Technology Components:** Different processes must be considered to effectively mitigate the risk of legacy or unsupported systems while updating systems or system components. *See* NIST SP 800-53. With respect to open source products, the Open Group[21] has created a set of standards and certification processes titled the "Trusted Technology Provider Standard (O-TTPS) Certification Program" to address supply chain controls for purchasers.
- **Supplier Relationships:** An important aspect of managing suppliers is knowing how to terminate relationships with third parties in a manner that limits the operational impact of losing the product or service. Such considerations are addressed in the Utilities Telecom Council white paper, *Supply Chain Risk Management for Utilities – Roadmap for Implementation.*[22]

While each of these industry standards and best practices can be informative, NERC has identified several best practices as particularly pertinent in addressing the supply chain risks faced by the electric power industry. NERC staff therefore recommends that entities adopt the following practices when developing their supply chain risk management programs:

- **Secure Hardware Delivery:** Many Cyber Assets purchased and deployed on the BES are hardware appliances configured to perform very specific real-time functions; these appliances may possess code that can be manipulated to cause them to potentially affect the reliable operation of the BES. Instituting hardware delivery controls like those described by the DOE Energy Sector Control Systems Working Group may help to reduce the risks if those devices are compromised in transport.
- **Third-Party Accreditation Processes:** Entities should include an independent assessment or third-party accreditation process of their vendors as part of their supply chain risk management strategy as identified in the APPA/NRECA and NATF white papers.[23] NERC will work with stakeholders to develop an accreditation

[19] NATF White Paper at 8–9.
[20] *Id*. at 18.
[21] The Open Group describes itself as a "global consortium that enables the achievement of business objectives through technology standards." The Open Group, https://www.opengroup.org/about-us/who-we-are.
[22] Utilities Telecom Council, Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation (Apr. 2015), available at https://utc.org/wp- content/uploads/2018/02/SupplyChain2015-2.pdf.
[23] *See* APPA/NRECA White Paper at 16; NATF White Paper at 13.

model for identifying vendors with strong supply chain risk management practices. Such identification would not only help entities increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cyber security controls and measures but also aid compliance with the proposed Reliability Standards. The process(es) for third party accreditation or certification should be developed and submitted to NERC for evaluation. Such process(es) should be implemented within 12 months of the effective date of Reliability Standard CIP-013-1.

- **Threat-Informed Procurement Language:** Entities should tailor their security specifications to the specific risks of their environment. This can be accomplished through threat modeling, which is a process to ensure that all products have a threat model specific to the current development scope of the product. This ensures the risk of procurement of any application or systems is appropriately weighed against the risk of compromise to the overall health of the organization or the BES. For example, if an entity is procuring a new remote access system for its medium impact BES Cyber Systems, the threat model should reflect the impact of the remote access system's effect to the BES, and the procurement language for that purchase should be specified according to its specific risk and system-specific vulnerabilities.
- **Processes to Address Unsupported or Open-Sourced Technology Components:** Where patch sources for systems or components are no longer available, entities should develop a plan to mitigate potential risks posed by these unsupported systems. Entities should also implement controls when purchasing open source technology, including responsibility for ongoing support and patching. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline on appropriate controls.

Using Supply Chain Controls to Mitigate Common-Mode Vulnerabilities: The Supply Chain Standards require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure that supply chain risks are being managed through the procurement process. As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. Risks of common-mode vulnerabilities can be mitigated if supply chain security practices are applied uniformly across cyber asset types and BES Cyber System impact levels. Further study is needed to determine whether there is any reliability benefit to extending the Supply Chain Standards to low impact BES Cyber Systems.

Additional considerations and guidance for developing robust supply chain risk management programs are provided in the white papers and guidance prepared by the Forums and Associations.

Reliability Standards to Address Supply Chain Risks

As noted above, NERC developed the Supply Chain Standards to address the risks to reliability posed by supply chain concerns. These standards require that responsible entities afford certain supply chain protections to their higher risk assets. This section summarizes the Supply Chain Standards and how the present applicability of those standards fits in the broader risk-based framework of the CIP Reliability Standards.

The Framework of the NERC CIP Reliability Standards

The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats. This approach requires BES Cyber Systems or Facilities that could have the highest impact to the grid receive the highest level of protections. In other words, the level of controls required for protecting cyber systems is in proportion to the risk each system presents to reliable operation of the BPS. This approach was used to mitigate the risk of malicious actors targeting specific assets or electric power entities because of their potential impact to the grid.

This risk-based construct requires users, owners, and operators of the BES to identify those cyber systems (referred to as BES Cyber Systems) that could have an adverse effect on BES reliability if lost, compromised, or misused.[24] Using bright-line criteria, responsible entities must then categorize their BES Cyber Systems as high, medium, or low impact based on the risks they present to the grid if lost, compromised, or misused. Once these BES Cyber Systems are identified and categorized, the CIP Reliability Standards require responsible entities to, among other things, establish plans, protocols, and controls to protect those systems against a cyber or physical attack, train personnel on security matters, report security incidents, and recover from security events. The Supply Chain Standards will require responsible entities to take additional actions to address cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems.

NERC Supply Chain Standards

The Supply Chain Standards consist of new Reliability Standard CIP-013-1 (Supply Chain Risk Management) and revised Reliability Standards CIP-005-6 (Electronic Security Perimeter(s)) and CIP-010-3 (Configuration Change Management and Vulnerability Assessments). The Supply Chain Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Collectively, the Supply Chain Standard requirements do the following:

- Reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System (CIP-010-3 Requirement R1 Part 1.6 and CIP-013-1 Requirement R1 Part 1.2 address this concern)
- Address vendor remote access-related threats, including the threat of stolen vendor credentials used to access a BES Cyber System without the responsible entity's knowledge as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System (CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-013-1 Requirement R1 Part 1.2 address this concern)
- Address the risk that responsible entities could unintentionally plan to procure and install vulnerable equipment or software within their information systems or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions (CIP-013-1 Requirement R1 Part 1.1 addresses this concern)
- Address the risk that responsible entities could enter into contracts with vendors who pose significant risks to their information systems as well as the risk that products procured by a responsible entity fail to meet minimum security criteria (CIP-013-1 Requirement R1 Parts 1.1 and 1.2 addresses this concern)
- Address the risk that a compromised vendor would not provide adequate notice of security events and vulnerabilities and related incident response to responsible entities with whom that vendor is connected (CIP-013-1 Requirement R1 Parts 1.2.1 and 1.2.2 addresses this concern)

Consistent with the general risk-based framework of the CIP Reliability Standards, the Supply Chain Standards are subject only to defined categories of Cyber Assets and BES Cyber Systems. **Table 1.1** summarizes the applicability of the Supply Chain Standards.

[24] BES Cyber Systems consist of one or more BES Cyber Assets, which the NERC Glossary defines as follows:

> "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems."

Table 1.1: Supply Chain Standard Applicability			
Requirement	**CIP-013-1**	**CIP-005-6 R2.4**	**CIP-010-3 R1.6**
High Impact BES Cyber Systems	✓	✓	✓
Protected Cyber Asset associated with High Impact BES Cyber Systems		✓	
Physical Access Control Systems associated with High Impact BES Cyber Systems			
EACMSs associated with High Impact BES Cyber Systems			
Medium Impact BES Cyber Systems[25]	✓	✓	✓
Protected Cyber Assets associated with Medium Impact BES Cyber Systems		✓	
Physical Access Control Systems associated with Medium Impact BES Cyber Systems			
EACMSs associated with Medium Impact BES Cyber Systems			
Low Impact BES Cyber Systems			

The Supply Chain Standards will require responsible entities to provide strong protections against the risks posed by supply chain compromise for those BES Cyber Systems and Protected Cyber Assets that are subject to the standards. As discussed in subsequent sections of this report, applying these protections more broadly would help reduce the supply chain risks inherent to categories of assets not currently subject to the standards.

Subsequent sections of this report address those assets not presently included in the Supply Chain Standards and the risks associated with those assets if compromised in the supply chain. Chapter 2 addresses EACMSs; Chapter 3 addresses PACS; Chapter 4 addresses low impact BES Cyber Systems; and Chapter 5 addresses PCAs. After evaluating each type of asset and the overall risk environment, NERC makes recommendations for further actions to address those risks.

[25] Reliability Standard CIP-005-6 Requirement R2 Part 2.4 and Reliability Standard CIP-010-3 Requirement R1 Part 1.6 are applicable to "Medium Impact BES Cyber Systems with External Routable Connectivity" and their associated PCA.

Chapter 2: Electronic Access Control or Monitoring Systems

Overview

This chapter addresses reliability risks associated with the supply chain for EACMSs, which are not currently subject to the Supply Chain Standards.

EACMSs are defined in the *NERC Glossary of Terms* as follows:

> ***Electronic Access Control or Monitoring Systems (EACMSs)***: "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s)[26] or BES Cyber Systems. This includes Intermediate Systems."

The components that make up EACMSs are typically used to control access to, secure, and monitor critical systems on the BES, such as EMS/SCADA and microprocessor-based relays.

Examples of EACMSs include Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, active directory servers, and certificate authorities), security event monitoring systems, and intrusion detection systems.[27] EACMS components include firewalls, routers, layer three switches, intrusion-detection systems, log monitors, and access control systems.

As discussed in this chapter, the CIP Reliability Standards currently contain protections for EACMSs. These protections, however, do not extend to risks specific to the supply chain. Because certain EACMSs components could have a real-time impact on the reliability of the BES if compromised, misused, or rendered unavailable, and consistent with FERC's Order No. 850 directive,[28] NERC staff recommends revising the Supply Chain Standards to address EACMSs. Specifically, NERC staff recommends revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with EACMSs that provide electronic access (excluding monitoring and logging) to high and medium impact BES Cyber Systems. That is, an entity should perform a comprehensive CIP-013-1 Requirement 1 Part R1.1 risk identification and assessment process to consider the potential impact of EACMSs within the entity's operating environment.

Current CIP Reliability Standard Protections for EACMSs

NERC has existing Reliability Standards that are applicable to EACMSs:

- Reliability Standard CIP-003-6 requires responsible entities to have policies that address cyber security for BES Cyber Systems, including EACMSs for high and medium impact BES Cyber Systems and electronic access controls for low impact BES Cyber Systems.
- Reliability Standard CIP-004-6 requires responsible entities to implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities for those individuals that have access to high and medium impact BES Cyber Systems and associated EACMSs. It also requires responsible entities to implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to high and medium impact BES Cyber Systems and associated EACMSs. It further requires entities to implement one or more access management program(s)

[26] The NERC Glossary defines an Electronic Security Perimeter (ESP) as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."
[27] *See* Background, Reliability Standard CIP-002-5.
[28] Order No. 850 at P 30.

and access revocation program(s) applicable to high and medium impact BES Cyber Systems and associated EACMSs.

- Reliability Standard CIP-006-6 requires responsible entities to implement one or more documented physical security plan(s) and documented visitor control program(s) for high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-007-6 requires responsible entities to implement one or more documented processes(s) that address enabling and disabling ports and services for high and medium impact BES Cyber Systems and associated EACMSs. It also requires entities to implement one or more documented process(es) that address patch management and malicious code prevention applicable to high and medium impact BES Cyber Systems and associated EACMSs. It further requires entities to implement one or more documented process(es) that address security event monitoring and logging and system access controls applicable to high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-009-6 requires responsible entities to implement one or more documented recovery plan(s) for high and medium impact BES Cyber Systems and associated EACMSs. It also requires those entities to test and maintain the recovery plan(s).
- Reliability Standard CIP-010-2 requires responsible entities to implement one or more documented processes(s) that address configuration change management and configuration monitoring for high and medium impact BES Cyber Systems and associated EACMSs. It also requires responsible entities to perform vulnerability assessments applicable to high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-011-2 requires responsible entities to implement one or more documented information protection program(s) and BES Cyber Asset reuse and disposal process(es) for high and medium impact BES Cyber System and associated EACMSs.

These requirements work together to form a cohesive security protection for deployed EACMSs; however, they do not address the concerns specific to the supply chain discussed below.

Potential BES Risks Associated with EACMSs due to Supply Chain Concerns

EACMSs are potentially vulnerable to risks from the supply chain. If compromised, misused, or rendered unavailable, EACMS components could have a real-time impact on the reliability of the BES. The risks posed by supply chain vulnerabilities depend in large part on the specific configuration of the EACMSs, where the EACMS is deployed (i.e., at low, medium, or high impact BES Cyber System), and the extent to which certain compensating measures are employed.

EACMSs can consist of systems that perform electronic access control and systems that perform monitoring and logging functions. The reliability risks associated with compromise of electronic access control systems are higher than those associated with monitoring and logging functions.

If a component of an electronic access control EACMSs were to be compromised in the supply chain, such as through the introduction of an unauthorized “backdoor,” a malicious actor could access (or bar authorized users from accessing) systems that directly affect the operation of the BES. If the compromised EACMS controls electronic access to a medium or high impact BES Cyber System, this compromise could negatively impact the reliability of the BES.

If a component of a monitoring EACMS was compromised in the supply chain, such as through the introduction of malicious code, it could impact the ability of the owner to quickly detect, alert to, and respond to a cyber attack. It can also result in real-time access alarms being masked from those that are actively assessing reliability. If a component of a logging EACMS was compromised, it could hinder the ability to perform forensic analysis after active or attempted attacks.

Where EACMSs are configured on a single platform, the risk to all services, including access control, monitoring, and logging, share a single higher risk level if the management plane[29] of the single device is compromised or misused. This is because such devices control access to critical systems from a single point. Services required for access, authentication, monitoring, logging, detection, and alerting could be altered or misconfigured, blinding operators and security personnel to potential unauthorized access and introduction of malicious code to BES Cyber Systems within an ESP.

The risks posed by vendor-initiated remote access sessions, whether through interactive remote access or system-to-system remote access, also represent a significant vector for attack into the associated BES Cyber System through the EACMS.

In evaluating the risks posed by supply chain compromise of EACMSs, NERC staff considered that half of the market share of substation networking equipment is held by only two vendors, one of which has a 55 percent world-wide enterprise network market share in the corporate environment of many industries, including the electric power industry.[30] If a major vendor unknowingly supplied compromised networking equipment, and the compromise was then exploited to allow access to EACMSs controlling electronic access to medium or high impact BES Cyber Systems, the compromise could have widespread negative impacts on reliability.

The potential risks of supply chain compromise described above can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards, while others could be addressed in an entity's policies and procedures. For example, strict authorization and authentication, up to and including multi-factor authentication, can be used to limit the risk posed by local or remote access to the management services of an EACMS by owner or vendor personnel. Other technical controls that could be put in place to secure access and communications include the following: implementing strong password policies; implementing role-based access control; using authentication, authorization, and accounting services; implementing access control lists; encrypting remote access sessions; and using separate secured virtual local area networks for data and management traffic. Testing, verification, and validation of the architecture, configuration, and management access of EACMSs can also help ensure that EACMSs are implemented as designed, meet the expected security controls objectives, and protect BES Cyber Systems within a defined ESP.

While the technical controls mentioned above can provide some protections against certain compromises introduced in the supply chain, they do not address all potential risks. Given the potential adverse impacts that could be caused by a compromised EACMS, it is important to identify and assess supply chain vulnerabilities when procuring and configuring these systems.

Recommended Actions to Address the Risks

Noting that "the vulnerabilities associated with EACMS are well understood and appropriate for mitigation," FERC directed NERC in Order No. 850 to revise the Supply Chain Standards to include EACMSs.[31]

Upon evaluation of the supply chain-related risks associated with EACMSs, particularly those posed by compromise of electronic access functions, NERC staff recommends that the Supply Chain Standards be modified to include EACMSs that perform electronic access control for high and medium BES Cyber Systems.

Consistent with the risk-based framework of the CIP Reliability Standards, any future revision to the Supply Chain Standards should account for the fact that EACMSs present different risks based on the functions that they perform.

[29] "Management plane" refers to the part of the system that configures, monitors, and provides management, monitoring, and configuration services to all layers of the system.
[30] EPRI Interim Report, at Chapter 2.
[31] Order No. 850 at P 30.

As described above, the BES Cyber Systems that perform electronic access control would, if compromised, present a higher risk to reliability than a compromise of monitoring or logging systems. This is because these access control systems serve as "gatekeepers" to critical systems. Work is currently underway on Project 2016-02 Modifications to CIP Standards[32] to develop new defined terms that separate out EACMS functions so that appropriate controls can be placed around appropriate risks.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with EACMSs. Various risk assessment techniques are provided in the APPA/NRECA and NATF white papers. For example, entities should perform a comprehensive risk identification and assessment process under Reliability Standard CIP-013-1 Requirement R1.1 that would, at a minimum, consider the following EACMS factors within the entity's operating environment:[33]

- Identify the components that comprise the EACMSs (i.e., specific cyber asset types)
- Identify the vendor(s) for each EACMS device type
- Identify the functions each EACMS device type performs to protect reliability (i.e., firewall, router, switch, etc.)
- Identify and prioritize: the risks presented by each EACMS device type if compromised (e.g., a compromised firewall could allow unauthorized or malicious traffic[34]); and informed potential mitigating circumstances (e.g., logging systems are primarily used for after-the-fact analysis rather than real-time protection)
- Assess the identified risks posed by each device type
- Develop potential strategies or recommendations to address and mitigate each identified risk
- Include recommendations to address EACMS risks in the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk as follows:
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, include recommendations relative to coordinated controls between the entity and applicable vendors associated with CIP-005-6 (Parts 2.4 and 2.5) for managing active vendor remote access sessions to and/or through EACMS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.5, include recommendations specific to planned methods associated with CIP-010-3 (Part 1.6) for verifying the identity of software sources and integrity of software obtained from such sources prior to application to EACMS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.6, include recommendations for controls specific to identified risks associated with compromised vendor-initiated remote access sessions

Reliability Standard CIP-013-1 Requirement 1 Part 1.2.5 addresses verifying the integrity and authenticity of software installed on particular assets. This verification helps to ensure that the software installed on high and medium BES Cyber Systems is not modified prior to installation without awareness of the software supplier and is not a counterfeit piece of software.

In the EACMS context, this software enables controls and monitoring. This highlights the importance of verification, especially for the "gatekeeping" monitoring assets. When the Supply Chain Standards are modified as recommended,

[32] Project 2016-02 Modifications to CIP Standards, http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

[33] This list is provided as an example of considerations for the CIP-013-1 Requirement R1.1 risk identification and assessment process, but it should not be considered an exhaustive or prescriptive list of all the variables that should be considered by each entity for EACMS within its unique operating environment.

[34] *See, e.g.*, EPRI Interim Report at 4-4.

the integrity and authenticity of the software installed on the particular assets that make up the system for monitoring and controlling would be covered by Reliability Standard CIP-013 Requirement 1 Part 1.2.5. This process would, in turn, support the verification required under Reliability Standard CIP-010-3, Requirement 1 Part 1.6. By verifying the integrity and authenticity of their EACMS software, entities can reduce the risk that software installed on the BES Cyber Systems (not just EACMSs, but all BES Cyber Systems) could be modified prior to installation without awareness of the software supplier or be a counterfeit piece of software.

Chapter 3: Physical Access Control Systems

Overview

This chapter addresses reliability risks associated with the supply chain for PACSs, which are not currently subject to the Supply Chain Standards.

PACSs are defined in the NERC *Glossary of Terms* as follows:

> ***Physical Access Control Systems (PACSs)***: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s),[35] exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers."

The systems that make up PACSs are often used to control and monitor physical access to Facilities and systems on the BES where BES Cyber Systems reside. These include physical intrusion-detection systems, log monitors, and systems to control physical access. Examples of PACSs cyber asset types include authentication servers, card systems, and badge control systems.[36]

As discussed in this chapter, the CIP Reliability Standards currently contain protections for PACSs. These protections, however, do not extend to supply chain risk management issues. To address these risks, NERC staff recommends revising the Supply Chain Standards to address those systems that provide physical access control, excluding alerting and logging. In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with PACSs. That is, an entity should perform a comprehensive Reliability Standard CIP-013-1 Requirement 1 Part R1.1 risk identification and assessment process to consider the potential impact of PACSs within the entity's operating environment.

Current CIP Protections for PACSs

NERC has existing Reliability Standards that are applicable to PACSs listed as follows:

- Reliability Standard CIP-003-6 requires responsible entities to have policies that address physical security for BES Cyber Systems, including PACSs for high and medium impact BES Cyber Assets and physical security controls for low impact BES Cyber Systems.
- Reliability Standard CIP-004-6 requires responsible entities to implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities for those individuals that have access to high and medium impact BES Cyber Systems and associated PACSs. It also requires entities to implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to high and medium impact BES Cyber Systems and associated PACSs. It further requires entities to implement one or more access management program(s) and access revocation program(s) applicable to high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-006-6 requires responsible entities to implement one or more documented physical security plan(s) and documented visitor control program(s) for high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-007-6 requires responsible entities to implement one or more documented processes(s) that address enabling and disabling ports and services for high and medium impact BES Cyber

[35] A PSP is defined in the NERC Glossary as "[t]he physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled."
[36] *See* Background, Reliability Standard CIP-002-5.

Systems and associated PACSs. It also requires entities to implement one or more documented process(es) that address patch management and malicious code prevention applicable to high and medium impact BES Cyber Systems and associated PACSs. It further requires entities to implement one or more documented process(es) that address security event monitoring and logging and system access controls applicable to high and medium impact BES Cyber Systems and associated PACSs.

- Reliability Standard CIP-009-6 requires responsible entities to implement one or more documented recovery plan(s) for high and medium impact BES Cyber Systems and associated PACSs. It also requires those entities to test and maintain the recovery plan(s).
- Reliability Standard CIP-010-2 requires responsible entities to implement one or more documented processes(s) that address configuration change management for high and medium impact BES Cyber Systems and associated PACSs. It also requires entities to perform vulnerability assessments applicable to high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-011-2 requires responsible entities to implement one or more documented information protection program(s) and BES Cyber Asset reuse and disposal process(es) for high and medium impact BES Cyber Systems and associated PACSs.

These requirements work together to form a cohesive security protection for deployed PACSs; however, supply chain concerns still exist and are further discussed in this chapter.

Potential BES Risks Associated with PACSs Due to Supply Chain Concerns

PACSs are potentially vulnerable to risks from the supply chain. If compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES. The risks posed by supply chain vulnerabilities depend in large part on the specific configuration of the PACS, where the PACS is deployed (i.e., at low, medium, or high impact BES Cyber System), and the extent to which certain compensating measures are employed.

Depending on specific configurations, PACSs could have a real-time impact on the reliability of the BES if compromised, misused, or rendered unavailable. Given this potential impact, it is important to consider supply chain vulnerabilities when procuring and configuring these systems.

A number of methods and systems may be used to control, monitor, and log physical access to BES Cyber Systems. These methods and systems are typically supplied at least in part by third parties and are thus vulnerable to compromises introduced in the supply chain.

Methods of physical access control include the following:

- **Card Key:** A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- **Special Locks:** These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- **Security Personnel:** Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- **Other Authentication Devices:** Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter (PSP).

- Methods to monitor physical access include the following:
  - **Alarm Systems:** Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
  - **Video Recording:** Electronic capture of video images of sufficient quality to monitor activity at or near PSPs and/or physical security access points.
  - **Human Observation of Access Points:** Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include the following:

- **Computerized Logging:** Electronic logs produced by the responsible entity's selected access control and alerting method.
- **Video Recording:** Electronic capture of video images of sufficient quality to determine identity.
- **Manual Logging:** A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

Similar to EACMSs, the PACS cyber systems that perform physical access control present a higher risk than monitoring and logging systems. A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios applicable to compromised PACS components (such as those described above) include, but are not limited to, the following:

- A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements could allow external threat actors to obtain undetected physical access to Control Centers and other Facilities that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems.
- Misuse, degradation, or destruction of PACS access control components could also allow internal threat actors to take adverse actions on BES Cyber Systems without detection. Such a scenario may precede a physical attack or support a subsequent cyber attack.

While not a specific supply chain risk, there is also a high potential for insider collusion with external threat actors to ensure PACS supply chain compromises are activated prior to a physical attack.

Compromise of the cyber systems that perform monitoring, while not presenting as high of a risk, could impact the ability to quickly analyze an attack and may mask real-time alarms for access from those that are actively assessing reliability. Compromised PACS monitoring systems may also eliminate the entity's ability to detect illicit access to Facilities and their associated BES Cyber Systems. A physical or cyber attack may be preceded by loss of capability to monitor for unauthorized access and to issue alarms or alerts to monitoring personnel, which may lengthen response times and allow threat actors to succeed in their attacks.

Compromise of logging systems would present a much smaller risk as these systems are used primarily to perform forensic analysis after active and potential attacks. Compromised PACS logging systems, however, could prevent accurate forensic analysis and potentially hamper recovery or restoration efforts.

The potential risks of supply chain compromise described above can be mitigated in part by controls, some of which are addressed in the CIP Reliability Standards while others can be addressed in entity policies and procedures. For example, strict operational or procedural controls can be used to limit the risk posed by unauthorized physical access

to BES Cyber Systems. Other controls that could be put in place to restrict access include implementing a completely enclosed "six-wall" boundary and implementing two or more different and complementary physical access controls. Testing, verification, and validation of the architecture, configuration, and management access of PACSs can also help ensure that PACSs are implemented as designed, meet the expected security controls objectives, and protect BES Cyber Systems within a defined PSP.

In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access.

However, given the potential adverse impacts that could be caused by compromised PACSs, particularly compromised access control systems, it is important to identify and assess supply chain vulnerabilities when procuring and configuring these systems.

Recommended Actions to Address the Risks

Upon evaluation of the supply chain-related risks associated with PACSs, particularly those that control physical access, NERC staff recommends that the Supply Chain Standards be modified to include PACSs that perform physical access controls for high and medium BES Cyber Systems.

Consistent with the risk-based framework of the CIP Reliability Standards, any future revision(s) to the Supply Chain Standards should account for the fact that PACSs present different risks based on the functions that they perform. As described above, the cyber systems that perform physical access control would, if compromised, present a higher risk to reliability than a compromise of alerting and logging systems.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with PACSs. Various risk assessment techniques are provided in the APPA/NRECA and NATF White Papers. For example, a comprehensive risk identification and assessment process under Reliability Standard CIP-013-1 Requirement R1.1 would, at a minimum, consider the following PACSs factors within the entity's operating environment:[37]

- Identify the components that comprise the PACSs (i.e., specific cyber asset types), including, but not limited to, the following:
  - Servers
  - Workstations
  - Cameras and other surveillance equipment
  - Access control cyber asset components
  - Monitoring components
  - Logging components
- Identify the vendor(s) for each PACS device type
- Identify the functions each PACS device type performs to protect reliability (e.g., authorizing and granting access, detection, response, monitoring, logging, etc.)

[37] This list is provided as an example of considerations for the CIP-013-1 Requirement R1.1 risk identification and assessment process, but it should not be considered an exhaustive or prescriptive list of all the variables that should be considered by each entity relative to supply chain risk management risks associated with PACS cyber asset types within its unique operating environment.

- Identify and prioritize the risks presented by each PACS device type if compromised (i.e., a compromised access authorization system could allow unauthorized or malicious access)
- Identify potential mitigating circumstances (i.e., logging systems are primarily used for after-the-fact analysis rather than real-time protection)
- Assess the identified risks posed by each device type
- Develop potential strategies and/or recommendations to address and mitigate each identified risk
- Include recommendations to address PACS risks the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk:
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.1, R1.2.2, and R1.2.4, entities may include physical security mitigation plans to minimize threats associated with such notifications and disclosures (e.g., increase guard force personnel to provide manual physical access controls at PSP Entry Points until such identified vulnerabilities are addressed)
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, integrate recommendations relative to coordinated controls between the entity and applicable vendors for managing physical access and active vendor remote access sessions to and/or through PACS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.5, integrate recommendations specific to planned methods associated with CIP-010-3 (Part 1.6) for verifying the identity of software sources and integrity of software obtained from such sources prior to application to PACS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.6, integrate recommendations for controls specific to identified risks associated with compromised vendor-initiated remote access sessions

Chapter 4: Low Impact BES Cyber Systems

Overview

Under the CIP-002 standard, responsible entities are required to categorize their BES Cyber Systems as either high, medium, or low impact using the bright-line impact rating criteria (IRC) outlined in Attachment 1 to the standard, as follows:

- Section 1 identifies the IRC for high impact BES Cyber Systems. The IRC is limited to BES Cyber Systems associated with four categories of Control Centers (*see* IRC 1.1–1.4).
- Section 2 identifies medium impact BES Cyber Systems associated with Control Centers, generation and transmission Facilities as well as specified remedial action and load shedding schemes (*see* IRC 2.1–2.13).
- Section 3 identifies BES Cyber Systems located at all other BES assets that were not previously identified under Sections 1 or 2. These low impact BES Cyber Systems are associated with smaller BES Facilities, such as Control Centers, generation and transmission Facilities, systems and Facilities critical to system restoration, specified transmission protection systems, including certain system protection and restoration systems owned by Distribution Providers (*see* IRC 3.1–3.6).

The Supply Chain Standards are applicable only to high and medium impact BES Cyber Systems.

In 2016, registered entities were requested to report the number of BES assets (e.g., Control Center, backup Control Center, substation, generation plant, etc.) identified in CIP-002-5.1 Requirement R1, Attachment 1 with high, medium, and low impact BES Cyber Systems as of July 1, 2016. Based on the results, NERC determined that approximately 21 percent of NERC registered entities own high or medium impact BES Cyber Systems; the remainder own only low impact BES Cyber Systems. It is important to note, however, that these survey results do not represent the percentage of assets containing low impact BES Cyber Systems. Many of the 21 percent of registered entities that own and/or operate high and medium impact BES Cyber Systems also own and operate a significant number of low impact BES Cyber Systems. Thus, additional data is needed to gauge the percentage of assets containing low impact BES Cyber Systems that are owned or operated by registered entities that also own medium and high impact BES Cyber Systems. Further study will help assess the residual risk to BES reliability associated with entities that own only low impact BES Cyber Systems.

NERC staff recommends further study of this issue as discussed below to determine whether the inclusion of low impact BES Cyber Systems with External Routable Connectivity should be considered while taking into account the number and nature of such low impact BES Cyber Systems, the benefits of including such systems in the Supply Chain Standards, and the associated costs of extending CIP-013 to cover these systems. While this work is underway, NERC staff recommends that the CIPC Supply Chain Working Group develop a guideline to assist entities in applying supply chain risk management plans to low impact BES Cyber Systems.

Supply Chain Risks Associated with Low Impact BES Cyber Systems

Low impact BES Cyber Systems are generally comprised of the same types of cyber assets as those in high and medium impact BES Cyber Systems and are therefore subject to similar supply chain risks, but individually present a lower risk to BES reliability if they are compromised. For example, these supply chain risks would include those posed by the introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems. These two risks have been cited by NRECA and APPA as two of the most significant supply chain risks facing their member entities.[38]

[38] APPA/NRECA white paper at 2.

The applicability of the Supply Chain Standards is consistent with the overall framework of the CIP Reliability Standards discussed above, which is to focus entity attention and resources on those assets that could pose the greatest risks to reliability if they were to be compromised. Low impact BES Cyber Systems are typically associated with isolated, smaller Facilities that are not currently subject to most[39] of the CIP Reliability Standards. Although compromise of an individual low impact BES Cyber System would, by definition, not pose a risk to reliability, the *EPRI Interim Report*[40] highlighted the potential negative impacts on reliability if numerous low impact BES Cyber Systems were compromised. This could happen if a major vendor with sizeable market share unintentionally supplied a compromised product to a sizeable percentage of the industry, and a malicious actor then exploited the single configuration-based vulnerability across a number of devices. Viruses, worms, and malware programs target "common mode vulnerabilities" in this manner.

To better understand this potential risk, EPRI conducted a market data analysis. This analysis consisted of assessing the product/manufacturer types used on the BES for SCADA/control systems, network and telecommunications, and operating systems. While this analysis does not break out the percentages of vendors supplying only low impact BES Cyber Systems, the information is useful as a general representation of the current state of the market. EPRI's analysis showed that two vendors, when combined, have half of the market share of substation networking equipment. It also showed the dominance of the Windows operating system in deployed systems. A further look at the data showed that a significant number of systems were running outdated (unsupported) operating systems and/or open operating systems. Also, two vendors, when combined, hold 82 percent of the existing deployment of energy management systems. By contrast, EPRI determined that no single vendor in the market for remote terminal units exceeded 20 percent market share.[41]

The risk to reliability posed by the mass exploit of a "common mode vulnerability" introduced in the supply chain for low impact BES Cyber Systems may be mitigated by several factors. First, while many CIP Reliability Standards are not applicable to low impact BES Cyber Systems, applying basic cyber hygiene practices could limit the reach and impact of such an event. Examples of such practices include application whitelisting, patching, minimizing domain or local administrative privileges, and disabling local administrative accounts where they are unnecessary. Second, the Supply Chain Standards are expected to have a positive impact on the overall market for electric industry goods and services, which would ultimately reduce the supply chain risks associated with low impact BES Cyber Systems. As noted in the APPA/NRECA White Paper, smaller entities that own only low impact BES Cyber Systems often purchase from the same, well-established vendors that larger entities with higher risk assets use. As larger entities with medium and high impact BES Cyber Assets demand certain supply chain practices from vendors, vendors may choose to apply those supply chain practices to all of their products sold to the electric power industry.[42] The Supply Chain Standards would therefore provide protections to low impact BES Cyber Assets even though the standards do not specifically cover them.

There is a second potential risk associated with low impact BES Cyber Systems, particularly those owned by an entity that also owns high or medium BES Cyber Systems. The risk is that a malicious actor could target the supply chain for a low impact BES Cyber System and, assuming no other controls were in place, exploit that vulnerability to attack other systems owned by the same entity, including high and medium BES Cyber Systems at larger and more critical BES Facilities including Control Centers, generation plants, and transmission Facilities.

[39] Effective January 1, 2020, Reliability Standard CIP-003-7 will be applicable to low impact BES Cyber Systems; Requirements R1.2 and R2 will require certain programmatic, physical, and electronic access protections.

[40] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").

[41] For more information on the specific market assessment, refer to the EPRI Interim Report at Chapter 2.

[42] APPA/NRECA white paper at 9-10.

This risk is thought to be mitigated, in large part, by entity supply chain practices. During the standard development process for the Supply Chain Standards, several procurement professionals stated that, other than for specific projects, they typically order cyber asset types without regard to the final destination. For example, orders may be placed for warehouse stock. A comprehensive Reliability Standard CIP-013-1 Requirement R1 supply chain risk management procurement plan that addresses all cyber asset types used by a registered entity in its high and medium impact BES Cyber Systems would also reduce comparable supply chain cyber security risks for assets deployed in low impact BES Cyber Systems.

Recommended Actions to Address the Risks

As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. This would help reduce the residual risks arising from the supply chain to those systems. Any cyber asset types identified as exclusive to low impact BES Cyber Systems should be evaluated on a case-by-case basis to determine the impact and extent of any supply chain risk management risks, which, if realized, could present a significant threat to the reliability of the BES. For entities that own both low and medium or high impact BES Cyber Systems, applying such practices to all assets regardless of destination would not only reduce the risks to its low impact BES Cyber Systems, but would also help streamline procurement and deployment processes generally.

NERC staff expects entities that own only low impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities. The APPA/NRECA white paper[43] provides considerations for smaller entities in developing such programs. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

For several reasons, NERC staff does not recommend revising the Supply Chain Standards to require protections for all low impact BES Cyber Systems at this time. The risk-based approach used in the CIP Reliability Standards generally, and the Supply Chain Standards specifically, enables responsible entities to prioritize controls for high and medium impact BES Cyber Assets. High and medium impact BES Cyber Systems as categorized in CIP-002 generally describe assets that are critical to interconnected operations, including transmission operations, reliability coordination, and balancing functions. CIP-013-1 provides responsible entities with flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. This approach provides an opportunity for industry to take measured steps to address complex supply chain cyber security risks based on their system needs. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets.

As described above, the implementation of the Supply Chain Standards is expected to have broader, positive impacts on both vendor and entity supply chain practices. Practices adopted by vendors to satisfy purchasers of assets deployed in high and medium BES Cyber Systems may ultimately be extended to assets deployed in low impact BES Cyber Systems as well. Following implementation of the Supply Chain Standards, NERC may find that there is no incremental reliability benefit associated with extending the Supply Chain Standards to low impact BES Cyber Systems.

Further, extending the Supply Chain Standards to low impact BES Cyber Systems could have unintended effects that may inadvertently increase the risk of common-mode vulnerabilities due to the reduction in diversity of vendors. For example, some vendors may choose not to provide small entities with the services required by the standards, such

[43] APPA/NRECA, *Managing Cyber Supply Chain Risk – Best Practices for Small Entities* (Apr. 25, 2018), https://www.cooperative.com/programs-services/government-relations/regulatory-issues/documents/supply%20chain%20white%20paper%204-25%20final.pdf ("APPA/NRECA White Paper").

as providing notification of vendor identified incidents that pose a cyber risk to the small entity, and owners of low impact BES Cyber Systems may thus have a smaller pool of potential vendors from which to choose. This smaller vendor pool could result in an increased risk that a common mode vulnerability in any one vendor's products or services could affect a substantial number of low impact BES Cyber Systems. Further study is necessary to determine the costs, reliability benefits, and potential unintended consequences of extending the Supply Chain Standards to low impact BES Cyber Systems.

Nevertheless, given the potential risk of a common mode vulnerability affecting numerous low impact BES Cyber Systems, NERC staff recommends further study to determine whether low impact BES Cyber Systems with External Routable Connectivity should be included within the scope of CIP-013. External Routable Connectivity is defined in the NERC Glossary as follows:

> "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."

Given this connectivity, these low impact BES Cyber Systems may pose a higher risk that could warrant mandatory supply chain protections.

First, NERC staff will propose to the Board a Request for Data or Information under Section 1600 of the NERC Rules of Procedure to obtain more information about the nature and number of BES Cyber Systems currently in use. NERC staff will work with the CIPC Supply Chain Working Group to determine the appropriate scope of the request. NERC staff expects that the request would address, at a minimum, the following considerations:

- The approximate total number of BES Cyber Assets in high/medium impact BES Cyber System(s): Of this number, the approximate number that have External Routable Connectivity
- The approximate total number of BES Cyber Assets in low impact BES Cyber Systems: Of this number, the approximate number that have External Routable Connectivity
- Questions to determine incremental costs and potential benefits to extend CIP-013 to low impact BES Cyber Systems with External Routable Connectivity:
    - The costs and potential benefits for entities that have high/medium impact BES Cyber Systems
    - The costs and potential benefits for entities that have only low impact BES Cyber Systems

Following the collection of the data, NERC staff will provide the results of the data analysis to industry.

Second, NERC staff will monitor the issue through the use of industry surveys and questionnaires following the implementation of the Supply Chain Standards to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity and to determine if there is consistent application of the criteria in CIP Reliability Standards that differentiate medium impact BES Cyber Systems from low impact. This new information would include actual market and entity practices following implementation of the Supply Chain Standards and the extent to which these practices may help reduce risks to reliability stemming from the supply chains for low impact BES Cyber Systems, including those with External Routable Connectivity. With this information, NERC and its stakeholders may make an informed analysis of whether mandatory requirements for all or a subset of low impact BES Cyber Systems are appropriate while taking into account the costs, expected benefits, and all other relevant considerations. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.

Chapter 5: Protected Cyber Assets

Overview

This chapter addresses the supply chain risk management risks posed by PCAs, which are currently subject to only a limited subset of the Supply Chain Standards.

PCAs are defined in the NERC Glossary of Terms as follows:

> ***Protected Cyber Assets (PCAs)***: "One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP."

Since there is a wide range of assets that fall under the category of PCAs, it is not possible to clearly define a general risk to the BES in the event they are compromised due to supply chain vulnerabilities. NERC staff recommends that entities, as a best cyber security practice, evaluate each PCA type on a case-by-case basis to identify any specific risks associated with supply chain risk management. This evaluation will allow each entity to determine whether supply chain risk management procurement processes are needed to mitigate the risk to associated BES Cyber Systems. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

Potential BES Risks Associated with PCAs due to Supply Chain Concerns

It is difficult to provide a general assessment of the risks that supply chain-compromised PCAs could present to the BES. By definition, PCAs do not represent an immediate 15-minute adverse impact to the reliability of the BES. PCA types, however, are sometimes identical to those cyber asset types identified as BES Cyber Assets. As a result, supply chain risk management practices should be highly dependent on the specific function of the PCA in question and the exposure risk to the BES Cyber Systems in the same ESP.

Overall PCAs are cyber assets most likely to be typical information technology assets like workstations, servers, printers, scanners, and other peripherals that support the work of operators and staff in the Control Center, data center, or security operations center environment. Based on type and configurations, PCAs could have the same risk profile of BES Cyber Assets associated with a high or medium BES Cyber System. Compounding the risk is that these systems may reside on the same network segments as a BES Cyber System while not being part of the BES Cyber System. Due to the potential interconnectedness of the PCA with the BES Cyber System, a compromise or misuse of the PCA could pivot to the BES Cyber System. The potential risk can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards and others which can be addressed in policies and procedures. For example, implementing access control lists, intrusion prevention systems, and malicious software prevention tools can be used to limit the risk posed by PCAs possibly impacting interconnected BES Cyber Systems.

Recommended Actions to Address the Risks

As a best practice, NERC staff recommends that entities evaluate each PCA type on a case-by-case basis to identify any specific risks associated with supply chain risk management and to determine whether supply chain risk management procurement processes are needed to mitigate risks to associated BES Cyber Systems. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

Entities should seek assurance that hardware or software components for PCAs are authentic and have not been modified prior to provisioning the PCA and when deploying required operational or security updates. Approved configuration management and change management processes should be followed for PCAs. A best practice would be to also include PCAs in a registered entity's baselining program to track and monitor the state of PCAs within their critical infrastructure networks.

Since PCAs are often the same cyber asset type as many common BES Cyber Assets, they may be subject to "common mode vulnerabilities" and represent an attack vector to BES Cyber Systems contained within the same ESP as the PCA. A comprehensive CIP-013-1 Requirement R1 supply chain cyber security risk management plan could be effective to support mitigation of PCA cyber assets obtained under the same supply chain risk management procurement plan as BES Cyber Systems associated with high and medium impact BES Cyber Systems. The specific processes should be made on a case-by-case basis after evaluating the potential risks associated with the supply chain for that device.

NERC staff does not recommend revising the Supply Chain Standards at this time to include PCAs. While PCAs are on the same network as BES Cyber Systems, other controls deployed on the BES Cyber Systems under the CIP-007 and CIP-010 standards would protect the actual assets that could have a 15-minute impact if rendered unavailable, degraded, or misused. Since there is a wide range of assets that fall under the category of PCA, the case-by-case approach described above would provide a flexible and cost effective approach to addressing supply chain risks associated with specific PCAs while avoiding unnecessary regulatory burden.

Chapter 6: Conclusion

Compromise of certain cyber assets in the supply chain could pose a threat to BES reliability. The Supply Chain Standards require responsible entities that possess high and medium impact BES Cyber Systems develop processes to ensure that supply chain risks are being managed through the procurement process. The Supply Chain Standards will be applied to the higher-risk systems that have the greatest impact to the grid.

NERC staff recommends that the Supply Chain Standards be modified to include certain assets associated with high and medium impact BES Cyber Systems in light of the risks that may be posed by compromise of such devices in the supply chain. In light of the risks posed by compromise of such devices, and to address FERC's Order No. 850 directive, NERC staff recommends revising the Supply Chain Standards to address EACMSs. Specifically, NERC staff recommends revising the standard to include EACMSs that provide electronic access control (excluding monitoring and logging). NERC staff also recommends revising the Supply Chain Standards to include PACSs that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. In the interim, NERC staff expects that entities will apply supply chain security practices to EACMSs and PACSs to help mitigate supply chain risks associated with these devices.

At this time, NERC staff does not recommend that the Supply Chain Standards be modified to include all low impact BES Cyber Systems. As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems to ensure risks are identified and assessed without regard for the ultimate destination of such common cyber assets. Additional consideration may need to be given to processes used by vendors and entities to mitigate supply chain risk to lower impact systems. Risks of common-mode vulnerabilities, as described in Chapter 4, can be mitigated if supply chain security practices are applied uniformly across cyber asset types and BES Cyber System impact levels. Further study is needed, however, to determine whether there is any reliability benefit to extending the Supply Chain Standards to low impact BES Cyber Systems.

NERC staff expects entities that own only low impact BES Cyber Systems will develop supply chain risk management programs tailored to their unique risk profiles and priorities. The APPA/NRECA white paper provides considerations for smaller entities in developing such programs. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

Due to the wide variation in risks associated with PCAs and mitigating controls already in place, NERC staff does not recommend that the Supply Chain Standards be modified to further address PCAs. NERC staff does, however, recommend that entities evaluate the risks on a case-by-case basis and adopt supply chain controls as appropriate to address those risks. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

Applying Industry Practices and Guidelines

Chapter 1 identified several noteworthy supply chain risk management techniques that are not required by the CIP Reliability Standards. While these standards address many fundamental elements of effective processes to manage the risk of a supply chain, the following noteworthy approaches, if applied correctly, can reduce residual supply chain risks:

- **Independent Assessment or Third-Party Accreditation Processes:** Entities should verify that standardized processes and measures were achieved to mitigate supplier risks.

- **Secure Hardware Delivery:** Entities should take steps to ensure that hardware and software are protected during physical transport.
- **Threat-Informed Procurement Language:** Entities should tailor their security specifications to the specific risk of their environment.
- **Unsupported or Open-Sourced Technology Component Processes:** Entities should employ processes to mitigate residual risks for unsupported systems and for open source technology.
- **Using Supply Chain Controls to Mitigate Common-Mode Vulnerabilities:** Entities should voluntarily apply similar techniques to manage supply chain risks at lower impact levels.

NERC staff recommends entities include these practices in developing their supply chain risk management programs.

Going Forward

NERC will work through its existing processes with stakeholders to review NERC staff's recommendations in this report and determine appropriate follow up actions.

The following additional work should be undertaken to evaluate the recommendations included in this report:

- **Section 1600 Data Request:** NERC staff, working with the CIPC Supply Chain Working Group, will develop a Request for Information or Data under Section 1600 of the NERC Rules of Procedure in an expedited manner. The results of this request will inform whether low impact BES Cyber Systems with External Routable Connectivity should be included within the scope of CIP-013.
- **Security Guidelines:** NERC staff, working with the CIPC Supply Chain Working Group, will develop security guidelines to assist entities in managing supply chain risks for EACMSs, PACSs, PCAs and low impact BES Cyber Systems.
- **Practice Guides:** The ERO will develop CMEP practice guides to create clear expectations on the types of questions registered entities may expect regarding their low impact BES Cyber Assets and the supply chain risk management activities afforded to those assets.
- **Industry Surveys and Questionnaires to Help Identify and Assess Industry Practices**: Voluntary efforts to obtain risk data can be used to obtain information about the installed base of systems used on the BES, the procurement language in contracts negotiated with key vendors, and data describing which CIP applicable systems have benefited from procurement language stemming from the Supply Chain Standards. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.
- **Targeted Outreach to Vendors that Support the Reliability of the BES:** Various vendors support the secure operations of the BES. Next steps should consider coordinated outreach to vendors that have a high market share of supplied products and services to the BES to ensure that they have awareness to their products' potential impact to reliability and their customers' responsibility to meet the rigor required by the CIP Reliability Standards. It is encouraged that industry work with their vendor points of contacts to ensure that technical and contractual considerations are addressing the standards.
- **Development of Standardized Vendor Data Sheets:** One of the challenges identified during the analysis of information used to prepare this report was the availability of vendor supply chain practices. The CIPC is working to develop a document for vendors about the CIP Reliability Standards. Further consideration should be given to the creation of a standardized method to provide product and supply chain security facts and features regarding vendor capabilities to help mitigate supply chain risks.

- **Third Party Accreditation/Certification Processes**: Process(es) for third party accreditation or certification should be developed and submitted to NERC for evaluation. NERC will work with stakeholders to develop an accreditation model for identifying vendors with strong supply chain risk management practices. Such identification would not only help entities comply with the proposed Reliability Standards but also increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cyber security controls and measures. Such process(es) should be implemented within 12 months of the effective date of Reliability Standard CIP-013-1.
- **Independent Testing of Legacy Applications and Products**: As discussed in NERC's plan to address supply chain risks, partnerships with independent organizations used to test and communicate product vulnerabilities used on the BES will be a key activity going forward. Understanding known vulnerabilities of the installed base will support the industry's effort to become more effective in negotiating contracts and resolving security issues in the procurement of upgraded systems and implementation of greenfield systems.

Future Considerations

In developing this report, NERC has identified several issues that, while outside the scope of this report, should be considered as part of future evaluations of supply chain risks and the effectiveness of the Supply Chain Standards.

As technologies and attacks have advanced and become more complex, entities are expressing interest in partnering with outside and government security services. These includes services like NERC's Cyber Security Risk Information Sharing Program (CRISP), Cybersecurity for the Operational Technology Environment, and those of external vendors and internal monitoring centers. It may prove difficult to understand and manage any supply chain risks for these systems. However, these providers have visibility into emerging threats and trends that comes through their extensive collections of information. Analysis of this information can then be shared more broadly, improving the overall cyber security posture of the customers and reliability of the BES through early detection of compromise.

Under the current body of CIP Reliability Standards, using these types of security services (that may also include electronic access or monitoring) may bring all Cyber Assets involved into scope as an EACMS. This may discourage or even preclude entities from using these services based on the associated BES Cyber System level requirements of an EACMS. These limitations affect patching, baselines, and other requirements as outlined in the CIP Reliability Standards, and may also be impacted by the Supply Chain Standards. There is great value in correlating security events seen across those networks that could be expanded to include an entity's other non-BES Cyber Assets. This activity could be precluded or discouraged through the administration of the current CIP Reliability Standards.

Appendix A: Summary of Actions Taken to Support the NERC Board Resolutions on Supply Chain

Support Effective and Efficient Implementation

The Board requested NERC to commence preparations for implementation of the Supply Chain Standards by using similar methods during the CIP V5 transition and regularly report to the Board on those activities.

To support this action, NERC engaged in several activities. NERC created a Supply Chain Risk Mitigation Program webpage to provide a single source for resources. The CIPC has established an advisory task force to provide input on activities to support standard implementation (e.g., webinars, workshops, and technical conferences) in coordination with NERC and the Regional Entities. Efforts are also underway to document existing risks and develop security guidelines for use by industry in managing known supply chain risks.

NERC and the Regional Entities hosted several small group advisory sessions with registered entities and NERC standards developers to discuss the preparation for and implementation of the Supply Chain Standards. Each session consisted of closed one-on-one discussions between a registered entity's supply chain security experts and ERO Enterprise staff about concerns pertinent to the entity's implementation of the proposed Supply Chain Standards. These sessions resulted in the development of a Frequently Asked Questions document.[44] The document addresses many of the questions and concerns voiced during those sessions.

In addition, NERC and the Regional Entities presented on the Supply Chain Standards and the security concerns regarding supply chain during regional workshops and outreach engagements. These presentations highlighted some of the costs regarding cyber attacks, risks identified in the EPRI Interim Report, and well-known public supply chain compromises. NERC also presented similar presentations to industry and other independent industry groups.

Going forward, NERC is considering additional small group advisory sessions and providing targeted outreach to entities and stakeholders.

In addition to actions taken to support the Board Resolutions, industry is also using existing NERC structures to improve reliability, security, and compliance. For instance, several prequalified organizations have already submitted compliance implementation guidance to support effective implementation of the Supply Chain Standards.

Cybersecurity Supply Chain Risk Study

The Board requested NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks. The interim report would be due 12 months after adoption of the resolutions and a follow-up final report would be due 18 months after adoption.

The following activities have occurred to support this action and are listed as follows:

- **Interim Report**
  - NERC contracted the Electric Power Research Institute to prepare an interim report on supply chain risks. The report focuses on the following areas:
    - An assessment of product/manufacturer types used on the BES
    - An analysis and applicability to BES Cyber Assets

[44] Frequently Asked Questions, Supply Chain – Small Group Advisory Sessions: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/SGAS%20FAQ%2006252018.pdf. (June 28, 2018).

  - An analysis of best practices and standards in other industries to mitigate supply chain risks
  - An analysis of generalized vendor practices and approaches used to mitigate supply chain risks
- NERC staff presented the interim report at the August 2018 Board meeting and posted the report on the Supply Chain Risk Mitigation Program webpage.

- **Final Report**

  This report, *Supply Chain Risks: Final Report and Recommended Actions*, was presented in draft to the Board in February 2019 and will be presented for acceptance to the Board in May 2019.

Communicate Supply Chain Risks to Industry

The Board requested NERC to communicate supply chain risk developments and risks to industry in connection with this report.

The following activities have occurred to support this action:

- NERC and E-ISAC have used NERC Alerts to communicate supply chain risks to industry.
- E-ISAC included a supply chain risk topic in NERC's Grid Security Exercise (GridEx IV).
- NERC and Regional Entities have included supply chain topics at workshops in 2018.
- CIPC is in the process of developing supply chain security guidelines.

Forum White Papers

The Board requested that the Forums (NATF and the NAGF) develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management as described in the resolution.

To support this action, the Forums have developed white papers, which are posted on the Supply Chain Risk Mitigation Program webpage.

Association White Papers

The Board requested that the Associations (NRECA and APPA) develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.

To support this action, the Associations jointly developed a white paper, which is posted on the Supply Chain Risk Mitigation Program webpage.

Evaluate Supply Chain Standard Effectiveness

The Board requested that NERC, collaborating with NERC technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board.

The plan to evaluate the effectiveness of the Supply Chain Standards will be developed by NERC staff in 2019, with assistance of the CIPC advisory group and Regional Entities.

Additional Information

NERC's Supply Chain Risk Mitigation Program webpage[45] provides more information on these and other ongoing efforts to support the implementation of the Supply Chain Standards and address ongoing supply chain considerations.

[45] NERC, Supply Chain Risk Mitigation Program: https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

Appendix B: CIPC Supply Chain Working Group Members

NERC wishes to take this opportunity thanks the following members of the CIPC Supply Chain Working Group and their organizations for their valuable contribution to this report.

Table B.1: CIPC Supply Chain Working Group

Member Name	Company
Amelia Anderson	CenterPoint Energy
Andy Bochman	IBM
Bob Lockhart	Utilities Technology Council
Brenda Davis	CPS Energy
Brian Bouyea	New York ISO
Brian Millard	Tennessee Valley Authority
Brian Tooley	Vectren
Celia Sieg	New York ISO
Chip Wenz	AES Corporation
Christopher Keane	Duke Energy
Christopher Plensdorf	DTE Energy
Christopher Walcutt	Direct Defense
Dalini Khemlani	Amazon Web Services
Darrell Klimitchek	South Texas Electric Cooperative
Darren Hulskotter	CPS Energy
David Godfrey	Garland Power & Light Company
David Jacoby	Boston Strategies International
David Sampson	DTE Energy
Donald Hargrove	Oklahoma Gas and Electric Co.
James Brown	California ISO
James Howard	Lakeland Electric
Jeffrey Kimmelman	Network and Security Technologies
Jerrod Montoya	Open Access Technology International
Jim McNierney	New York ISO

Table B.1: CIPC Supply Chain Working Group	
Member Name	**Company**
John Hochevar	American Transmission Company
Jose Flores	North American Transmission Forum
Joseph Smith	Public Service Enterprise Group
Kaitlin Brennan	Edison Electric Institute
Kara White	NRG
Karl Perman	EnergySec
Keith St. Amand	Midwest ISO
Ken Keels	North American Transmission Forum
Kevin Weber	Entergy
Lee Maurer	Oncor Electric Delivery
Marc Child	Great River Energy
Marina Rohnow	San Diego Gas and Electric
Mark Henry	Texas Reliability Entity
Matt Anglin	New York ISO
Michael Aukerman	Denton Municipal Electric
Michael Meason	Western Farmers Electric Cooperative
Mike Mertz	PNM Resources
Michele Wright	FoxGuard Solutions
Michelle Coon	Open Access Technology International
Mike Kraft	Basin Electric Power Cooperative
Mike Prescher	Black and Veatch
Monika Montez	California ISO
Nathan Shults	Kiewit Engineering and Design
Patricia Ireland	DTE Electric
Patricia Meara	Network and Security Technologies
Peter Nelson	Network and Security Technologies
Pierre Janse van Rensburg	ENMAX Power Corporation

Table B.1: CIPC Supply Chain Working Group	
Member Name	**Company**
Reed Thompson	Public Service Enterprise Group
Robert Koziy	Open Systems International
Ryan Carlson	Proven Compliance Solutions
Sarah Stevens	North American Transmission Forum
Scott Webb	Network and Security Technologies
Sharla Artz	Utilities Technology Council
Sheranee Nedd	Public Service Enterprise Group
Steen Fjalstad	Midwest Reliability Organization
Steve Brain	Dominion Energy
Steven Briggs	Tennessee Valley Authority
Tony Eddleman	Nebraska Public Power District

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-2

Supply Chain Risk Assessment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Risk Assessment

Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request

December 9, 2019

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

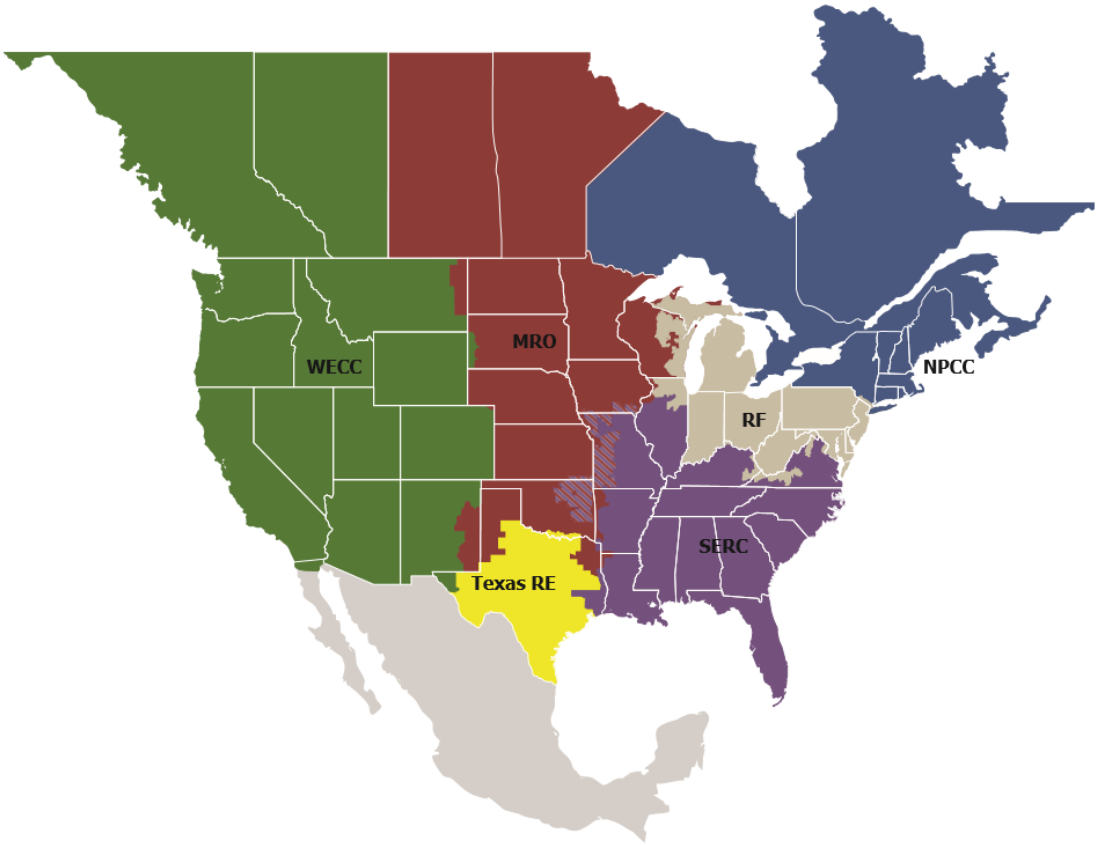
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Acknowledgements

In addition to the efforts of NERC staff, the success of any report depends largely on the guidance and input of many others. NERC wishes to take this opportunity to express a special thanks to Carter Manucy at the Florida Municipal Power Agency for his exceptional contributions to the analysis of the data in this report. NERC also wishes to take this opportunity to express a special thanks to the Critical Infrastructure Protection Committee Supply Chain Working Group for their valuable contribution to developing the Supply Chain Risk Assessment Data Request authorized by the NERC Board of Trustees (Board). The authors also acknowledge and appreciate the significant contributions from individuals, working groups, subject matter experts, and organizations whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this assessment.

Executive Summary

Recognizing the complex and evolving nature of supply chain risks, NERC has undertaken various efforts to identify and mitigate potential risks. In particular, information and communications technology and industrial control systems may provide opportunities for adversaries to initiate cyberattacks, thereby presenting security risks to the Bulk Electric System (BES).[1] NERC is committed to using its many reliability tools to support industry's efforts to mitigate supply chain risks.

The risk to the BES from supply chain vulnerabilities lies in the increasing dependence of owners and operators on microelectronics, computer networks, and telecommunications. Complex control systems (such as those employed in the electric power industry) have become more sophisticated and complex, enabling better responsive control of the BES. The NERC critical infrastructure protection (CIP) Reliability Standards employ an asset-centric, risk-based approach to securing the BES. This approach requires systems or facilities that have the highest impact to the grid receive the highest level of protections while the lowest impact systems receive the fewest security requirements. This approach serves to mitigate the risk of threat actors targeting individual assets or electric power entities because of their potential impact to the grid. However, threats originating from supply chain vulnerabilities may challenge this asset-centric approach. The impact to the reliability of the BES could be significant if multiple owners and operators allow third-party access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.

In 2017, NERC developed new and revised CIP Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards will be applicable to the highest-risk systems that have the greatest impact to the grid. The Supply Chain Standards will require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure responsible entities manage supply chain risks to those systems through the procurement process, thereby reducing the risk that supply chain compromise will negatively affect the BPS.

When adopting the Supply Chain Standards in August 2017, the NERC Board directed NERC to undertake further action on supply chain issues. Among other things, the Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards and develop recommendations for follow-up actions that will best address identified risks.

To better understand these risks, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure. This assessment documents the results of the analysis of the data to understand the implications of supply chain vulnerabilities not covered by the Supply Chain Standards and the extent of potential impacts (likelihood and risks to the BES). One observation was that most low impact assets reside in organizations with higher impact assets that are applicable to the approved Supply Chain Standards. This means that the low impact assets may be subject to the entity's supply chain risk management program and already have processes necessary to address supply chain vulnerabilities. However, many responders to the data request stated that their low impact BES Cyber Systems would be unaffected, especially for vendors that were not supplying high or medium impact BES Cyber Assets. The analysis is not aligned with the expectation in the NERC report that entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems.

[1] Unless otherwise indicated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

The analysis also showed that the vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at locations that have less than 500 MW. As such, an individual compromise to any one of these locations (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection wide BES reliability impact. One method to counter a coordinated cyberattack is to limit or eliminate third-party electronic access to these locations. Entities that have only low impact BES Cyber Systems allow third-party access to a significant number of their transmission stations and substations. While these locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could affect BES reliability beyond the local area. The analysis of third-party electronic access to generation resource locations is even more concerning. More than 50% of all low impact locations of generation resources allow third-party electronic access. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly affect BES reliability beyond the local area.

Based on this information and analysis of NERC's data request, NERC staff recommends modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

Background

In recent years, the Federal Energy Regulatory Commission (FERC), NERC, and industry identified risks from the supply chain as a potential threat to BES reliability. Supply chains for information and communications technology and industrial control systems are long and multidimensional and involve numerous parties in a multitude of countries across the globe. In procuring products and services for their operations, BPS owners and operators typically rely on vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. Malicious actors may target one or more vendors in the supply chain to create or exploit vulnerabilities that could then be used to initiate cyberattacks on BES Cyber Systems and equipment.

On July 21, 2016, FERC issued Order No. 829,[2] directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations:

> "[FERC directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[3]

Following the issuance of this order, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3.

The Supply Chain Standards support reliability by requiring responsible entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact BES Cyber Systems. Consistent with Order No. 829, the proposed Reliability Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Reliability Standard CIP-013-1 requires responsible entities to develop and implement plans to address supply chain cyber security risks during the planning and procurement of high and medium impact BES Cyber Systems. Modifications in CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.

The Board adopted the Supply Chain Standards at its August 10, 2017, meeting. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018.[4]

In its final report accepted by the NERC Board in May 2019,[5] NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and

[2] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards,* 156 FERC ¶ 61,050 (2016).
[3] *Id.* at P 2 (internal citation omitted); *see also id.* at PP 44–45.
[4] Order No. 850, *supra* note 1.
[5] NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 2019), available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity[6] by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure. NERC staff worked with the CIPC Supply Chain Working Group to develop the questions in the data request.

NERC issued the request for data or information[7] in accordance with the expedited timing provisions of Section 1606 of the NERC Rules of Procedure, as the information was needed to evaluate a threat to the reliability or security of the BPS. On June 13, 2019, the Board authorized the use of shortened review and comment periods. NERC provided the data request to the FERC Office of Electric Reliability for information on June 24, 2019 and posted for public comment for a 20-day comment period from July 2–July 22, 2019. The Board approved the formal issuance of this data request on August 15, 2019. In accordance with Section 1600 of the NERC Rules of Procedure, the data request was mandatory for U.S. entities. Although not required, Canadian registered entities were encouraged to participate. NERC collected the data from August 19 through November 3. The results of this data request and analysis are provided in the following chapters.

[6] In this context, the phrase "external connectivity" refers to inbound or outbound electronic access, as defined in CIP-003-7, Attachment 1, Section 3. This is not to be confused with External Routable Connectivity that applies to medium and high impact BES Cyber Systems.
[7] NERC's Supply Chain Risk Assessment Data Request:
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Final%201600%20data%20request%20-%20clean.pdf

Chapter 1: Summary of Data Request Questions

Supply Chain Risk Assessment Data Request

In its May 17, 2019, report titled *Cyber Security Supply Chain Risks – Staff Report and Recommended Actions,* (Supply Chain Report), NERC staff recommended issuing a data request under Section 1600 of the NERC Rules of Procedure "to obtain more information about the nature and number of BES Cyber Systems currently in use."[8] The Supply Chain Report states that the data request would include questions "to determine the incremental costs and potential benefits to extend CIP-013 to low impact BES Cyber Systems with External Routable Connectivity" (ERC).[9] NERC asked the following questions in the data request to achieve the objectives stated in the Supply Chain Report.

General Questions:

1. What are the NERC Compliance Registry numbers for which you are reporting under this Data Request?
2. Entity contact information
   a. Name:
   b. Title:
   c. Email address:
   d. Contact number:
3. CIP-002 Classifications.

CIP-002 Classifications	
Impact Rating	**Number of assets containing BES Cyber Systems**
High/Medium impact w/ ERC:	
Medium impact without ERC:	
Low impact:	
Low impact with external connectivity:[10]	

4. If you have medium or high impact BES Cyber Systems, please explain how your CIP-013-1 R1 plan will affect your low impact BES Cyber Systems and describe methods (if any) you intend to use to apply your plan to low impact BES Cyber Systems. In addition, have you determined if there are supply vendors used for acquiring low impact BES Cyber Assets that do not provide similar equipment or services to your high or medium impact BES Cyber Assets? If yes, please describe how you intend to address the risk:
5. If you have only low impact BES Cyber Systems, briefly explain how you currently plan on mitigating Supply Chain Management risks:

[8] Supply Chain Report at 20.
[9] *Id.*
[10] In this context, the phrase "external connectivity" refers to inbound or outbound electronic access, as defined in CIP-003-7, Attachment 1, Section 3. This is not to be confused with External Routable Connectivity that applies to medium and high impact BES Cyber Systems.

The following information was provided to assist in answering Questions 3–5:

> NERC needed to understand the basis for each entity's answer in order to understand the data received from the data request. How each entity categorized its BES Cyber Systems could have a large impact on survey results. To have useable and comparable results, the common basis was the six locations highlighted in CIP-002. The data request focused on those locations and not how entities designed their BES Cyber Systems.
>
> In the Supply Chain Report, NERC staff stated that they expected the following: entities that have medium or high impact BES Cyber Systems to voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems, and entities that own only low impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities.
>
> The term "location"[11] referred to physical space associated with an asset. A location includes any number of BES Cyber Systems at a given asset, as defined in CIP-002-5.1a, that operate at a common impact rating. For example, if a substation contains both medium and low impact BES Cyber Systems, the entity would include it in both counts. For Question 3, low impact count is all low impact assets containing BES Cyber Systems, including those with external connectivity. For each location in the response to Question 6, entities were to provide an estimate of the low impact assets identified pursuant to CIP-002 R 1.3.

6. For each location identified, answer the following questions. You may group assets with the same answers into a single line item. Note "inbound or outbound connectivity" refers to the requirements under CIP-003-7, Attachment 1, and Section 3. This is not to be confused with External Routable Connectivity that applies to medium and high impact BES Cyber Systems.

Low Impact Risk Assessment by Locations												
Impact Categorization BES Cyber Systems (See CIP-002, Attachment 1)	**3.1**			**3.2**			**3.3**			**3.4**	**3.5**	**3.6**
Location Risk Score[12]	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**2**	**1**
a. Number of locations with low impact BES Cyber Systems												
b. Number of locations with inbound or outbound connectivity to a BES Cyber System												
c. Number of locations with dial up												

[11] CIP-002-5.1a, Requirement R1 identifies six types of "assets" that entities must consider: (i) Control Centers and backup Control Centers; (ii) Transmission stations and substations; (iii) Generation resources; (iv) Systems and facilities critical to system restoration; (v) Special Protection Systems; (vi) for Distribution Providers, Protection Systems specified in CIP-002-5.1a, Applicability Section 4.2.1. For the purpose of this data request, the word "asset" is used in the same way as it is used in CIP-002-5.1a Requirement R1. The capitalized term "Cyber Asset" is used in this Data Request to have the same meaning as it has in the NERC Glossary of Terms.

[12] Risk score is based off of the value found in the "Location Risk Score Table" following

Low Impact Risk Assessment by Locations												
Impact Categorization BES Cyber Systems (See CIP-002, Attachment 1)	**3.1**			**3.2**			**3.3**			**3.4**	**3.5**	**3.6**
Location Risk Score[12]	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**2**	**1**
connectivity to a BES Cyber System												
d. Number of locations allowing third-party remote access[13] to a BES Cyber System												
e. Number of locations with third-party monitoring of a BES Cyber System[14]												
f. Number of locations with constant monitoring[15] of remote connectivity to a BES Cyber System												
g. Number of locations participating in government/industry programs[16]												
h. Number of locations with NO external routable connectivity and NO dial up connectivity to a BES Cyber System												

The following information was provided to assist in answering Question 6.

> To help NERC determine the risk to the BES associated with each of the locations containing low impact BES Cyber Systems, a scoring system based on the characteristics of the assets at that location was developed. Because low impact BES Cyber Systems are understood to pose some kind of risk to the BES, '1' is the lowest score on the scale. Neither the CIP Version 5 Reliability Standards nor the data request require entities to have an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets. To complete the data request related

[13] Access, for the purpose of this data request, means communication other than outward-bound data (e.g. a data diode that only sends data out of the location would not count).

[14] Third-party monitoring refers to connections that send data to an OEM or other third party that monitors components at this location for performance, maintenance, or other such reasons.

[15] Constant monitoring, for the purpose of this data request, means the ability to monitor connectivity and the ability to disconnect remote connectivity if malicious activity is detected.

[16] Government/Industry programs include, but are not limited to, CRISP, CYOTE, and/or Neighborhood Keeper. If a registered entity participates in one or more of these programs, they should only include the locations that are participating in the program. For example, do not count locations where the program(s) are applied only at a non-CIP environment (e.g., corporate).

to low impact BES Cyber Assets, an entity needed to only identify, to the best of its ability, the locations of low impact Cyber Assets and provide an approximate number of those locations. For each location containing different or multiple assets, they were instructed to use the first criterion that applies (i.e., count each location once) in the below table to determine its associated risk score.

Location Risk Score Table			
Criterion (See CIP-002 Attachment 1)	**Description**	**Risk Criterion**	**Location Risk Score**
3.1	Control Centers / backup Control Centers[17]	MW of load and/or generation controlled	0–500 MW = 2 501–1,000 MW = 3 1,001-1,500 MW = 4
3.2	Transmission stations and substations	MVA/Criterion 2.5 Score	0–1400 = 2 1,401–2,000 = 3 2,001–3,000 = 4
3.3	Generation resources[18]	MW per location	0–500 MW = 2 501–1,000 MW = 3 1,001–1,500 MW = 4
3.4	Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements[19] if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.5	SPS/RAS that support the reliable operation of the BES if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.6	For DPs, Protection Systems specified in Applicability section 4.2.1 if not counted in 3.2 or 3.3	All locations will receive the same score.	1

CIP-013 Cost of Implementation:
The following information was provided to assist entities in answering the questions after the information:

Stakeholders, regulators, and legislator's decisions on mitigating and preventing supply chain risks depend on the costs and benefits associated with those decisions. While utilities would want and share this information, it is not currently available. Therefore, subject matter experts believe it is premature for CIP-013 registered entities to determine or estimate costs or benefits associated with the implementation of the standard:

- The standard is new and there is no historic precedence for registered entities to pre-determine costs based on furthering relationships with existing and new vendors.

[17] These are low impact Control Centers per CIP-002-5.1a that only apply to some BAs and GOPs.
[18] If your entity has performed generation segmentation and created multiple low impact BES Cyber Systems, account for them as individual low impact BESCS locations (four units would count as four locations) as per your CIP-002. Do not double-count under medium impact under Question 3 and again as low impact under Question 5.
[19] If this includes generation counted under 3.3, do not count again under 3.4

- These costs and benefits are intangible and depend on a spectrum of actions, from internal process refinement costs to extensive costs associated with replacement of blacklisted vendors.
- The cost of compliance is currently unknown as this is a new standard.
- Many utilities are experiencing push back from vendors for CIP-013 compliance that could require vendor change or increase in cost from such vendors.

  Consequently, CIP-013 is causing and will necessitate many changes for complying utilities from now until the July 1, 2020, implementation date. Therefore, currently providing any credible cost or benefit information is premature.

7. Do you agree with the above SME assessment—Yes or No?

Provide CIP-013 cost or benefit amounts should you answer "no" to the above question:

Overview of Responses

This section provides an overview of the responses received from the data request.

Questions 1–3: NERC received responses from 1,040 entities.[20] 654 of these (63%) had only locations with low impact BES Cyber Assets with the remainder (386 or 37%) having a combination of locations that contained high, medium, and low impact BES Cyber Assets. The analysis of responses for question 3 is provided in Chapter 2.

Question 4: When those entities that had a combination of high, medium, and low impact BES Cyber Assets were asked about how their CIP-013-1 R1 plan will affect their low impact BES Cyber Systems, responses were mixed. Some stated that they plan to use a documented enterprise-wide supply chain cyber security risk management plan, which would include all Cyber Assets regardless of impact rating criteria. Others stated that their low impact BES Cyber Systems would be unaffected, especially for vendors that were not supplying high or medium impact BES Cyber Assets. This is contrary to the expectation in the Supply Chain Study that entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems.

Question 5: When those entities that had only low impact BES Cyber Assets were asked how they currently plan on mitigating Supply Chain Management risks, many stated that they would use only trusted vendors and/or develop a supply chain risk list. Many entities stated that the list would be developed by using a common risk assessment across those vendors. Others planned to rely on information from NERC's Electricity Information Sharing and Analysis Center to identify known vulnerabilities and potential supply chain issues. Many planned to control risk through processes developed for compliance with CIP-003. Some have taken the position that since no requirements exist mandating the mitigation of Supply Chain Management risks for low impact BES Cyber Systems, they do not intend to implement any plan to mitigate the risks. This lack of consistency on this risk assessment means that there is no certainty across industry that there are consistent supply chain protections. Therefore, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection wide BES reliability impact.

Question 6: The analysis of responses for question 6 is provided in Chapter 2.

Question 7: The Supply Chain Working Group developed a draft response to the cost to implement the Supply Chain Standards, which was provided in the data request and entities were asked if they agreed with the statement. More than 99% of the responders agreed with the draft response that it was premature for CIP-013 registered entities to

[20] While there are over 1,400 registered entities, many are not subject to the CIP standards and thus are not required to respond to the survey. The respondents represented those that were subject to the CIP standards.

determine or estimate costs or benefits associated with the implementation of the standard based on the list of factors provided.

Chapter 2: Analysis of Data

Comparison of BES Cyber Asset locations

NERC needed to understand the basis for each entity's answer in order to understand the data received from the data request. How each entity categorized its BES Cyber Systems could have a large impact on these survey results. For comparison and to have a common basis, NERC used the asset locations referenced in CIP-002-5.1.a:

i. Control Centers and backup Control Centers

ii. Transmission stations and substations

iii. Generation resources

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements

v. Special Protection Systems that support the reliable operation of the BES;

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1.

The data request focused on asset locations and not how entities designed their BES Cyber Systems.

Figure 2.1 provides a summary of the responses to question 3. Approximately 87% of all locations have low impact BES Cyber Systems, and many of those locations have external connectivity (defined as inbound or outbound electronic access) as defined in CIP-003-7, Attachment 1, Section 3. The BES Cyber Systems located at these locations would not be subject to the current Supply Chain Standards.

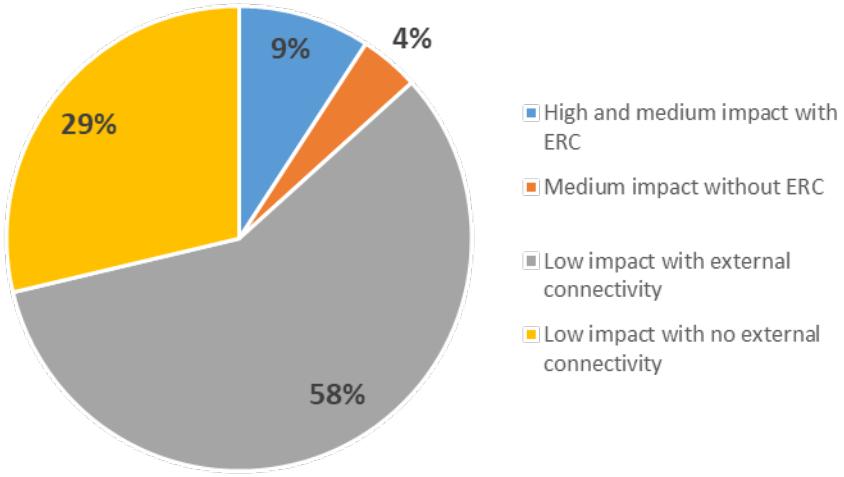


Figure 2.1: All Locations Containing BES Cyber Systems

NERC differentiated the responses based on entities that had a combination of locations of high, medium, and low impact BES Cyber Systems compared to entities that had only locations of low impact BES Cyber Systems. **Figure 2.2** shows the data for entities with a combination of locations. Note that the percentages are relatively close to those in **Figure 2.1**. In other words, most of the locations are at entities that have a combination of locations of high, medium, and low impact BES Cyber Systems. NERC then contrasted with responses from entities that had only locations of low impact BES Cyber Systems, which **Figure 2.3** shows. Note that two-thirds of these low impact BES Cyber Systems locations had external connectivity. In addition, when comparing connectivity across impact categories, the ratio of external connectivity to no external connectivity remained consistent at two-to-one.

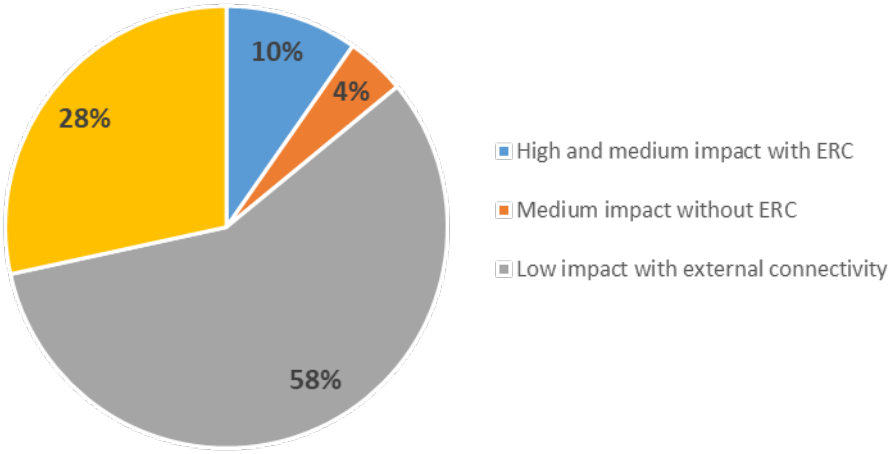


Figure 2.2: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

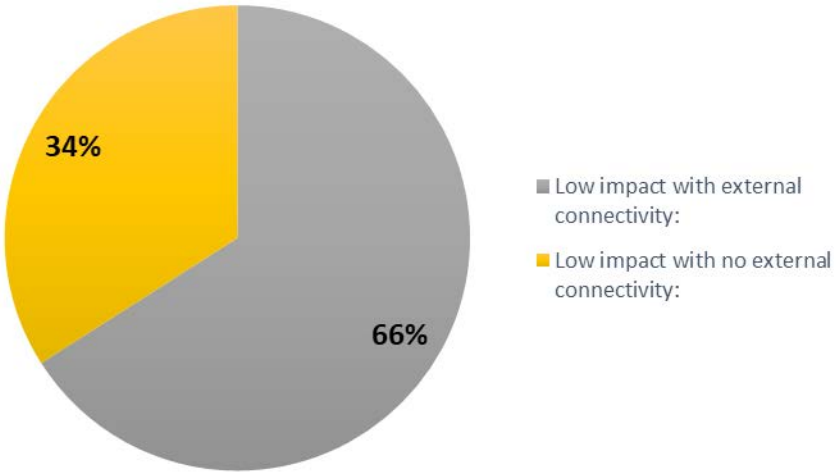


Figure 2.3: Locations for Entities with only Low Impact BES Cyber Systems

NERC then examined the data to determine whether entities allowed inbound or outbound connectivity at locations with low impact BES Cyber Systems. **Figure 2.4** shows the data for entities that have a combination of low, medium, and high impact BES Cyber Systems. The predominance of locations are transmission stations and substations as well as generation resources. In addition, a significant percentage of those entities allow inbound or outbound connectivity. **Figure 2.5** shows the data for entities that have only low impact BES Cyber Systems. Again, the predominance of locations are transmission stations and substations as well as generation resources, with a significant percentage of those locations allowing inbound or outbound connectivity. Further generation resources that allow inbound or outbound connectivity outnumber the transmission stations and substations in this dataset.

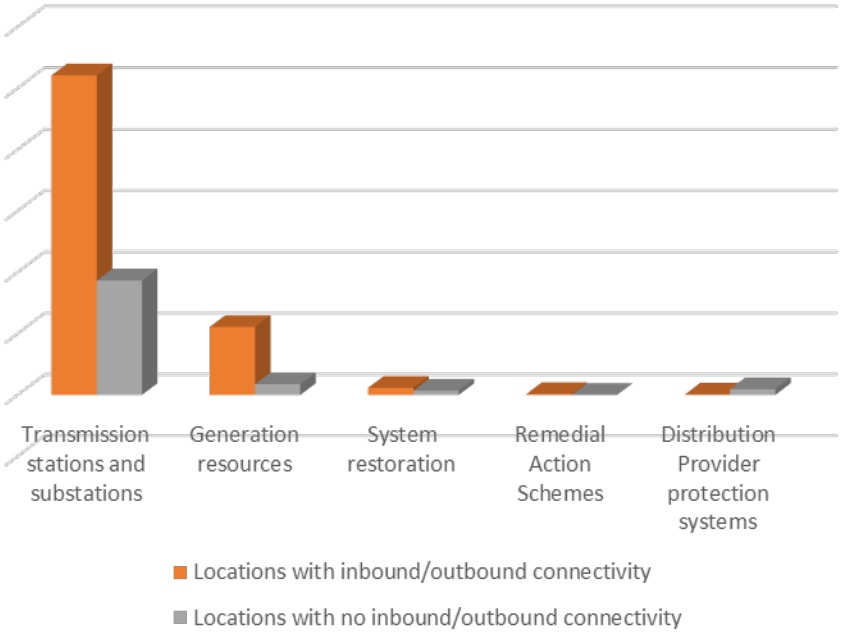


Figure 2.4: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

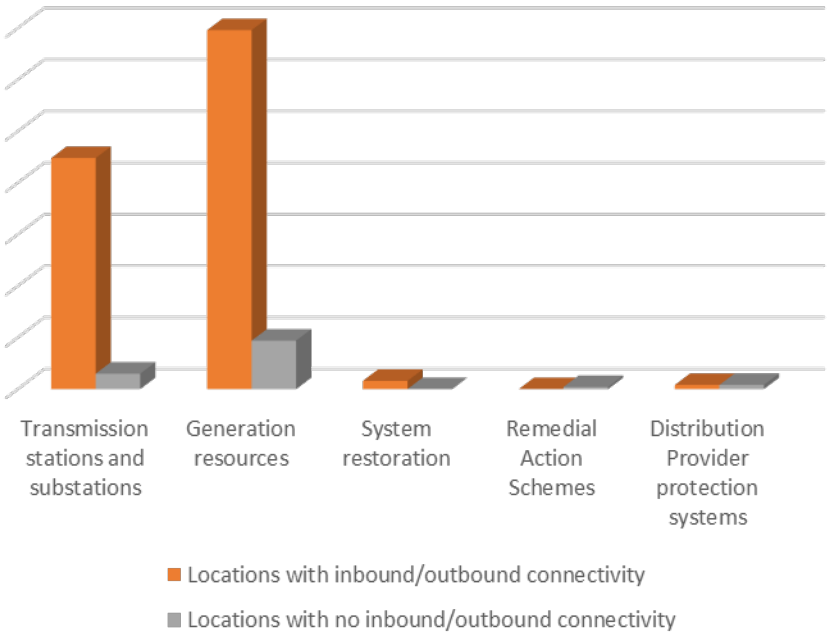


Figure 2.5: Locations for Entities with only Low Impact BES Cyber Systems

Since third-party access is a security risk, especially when it comes to supply chain vulnerabilities, NERC examined the data to determine whether an entity allowed third-party access at locations with low impact BES Cyber Systems. **Figure 2.6** shows the data for transmission stations and substations for entities that have a combination of low, medium, and high impact BES Cyber Systems. The vast majority of these locations do not allow third-party access, no matter the MVA criteria as established in criterion 3.2 in the data survey. **Figure 2.7** shows the data for transmission stations and substations for entities that have only low impact BES Cyber Systems. A significant percentage of these locations **do** allow third-party access, but only for the lowest location risk score as established in criterion 3.2 in the

data survey. In addition, while no values are presented in this report, the total number of locations represented in **Figure 2.7** represents only 3% of all transmission stations and substations locations reported low impact BES Cyber Systems. While these locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could impact BES reliability beyond the local area.

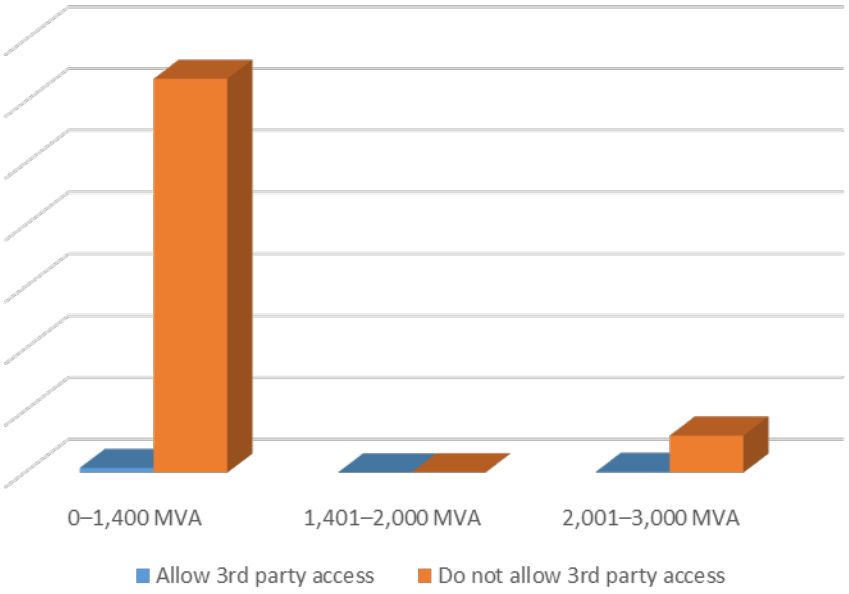


Figure 2.6: Transmission Stations and Substations for Entities with High, Medium, and Low Impact BES Cyber Systems

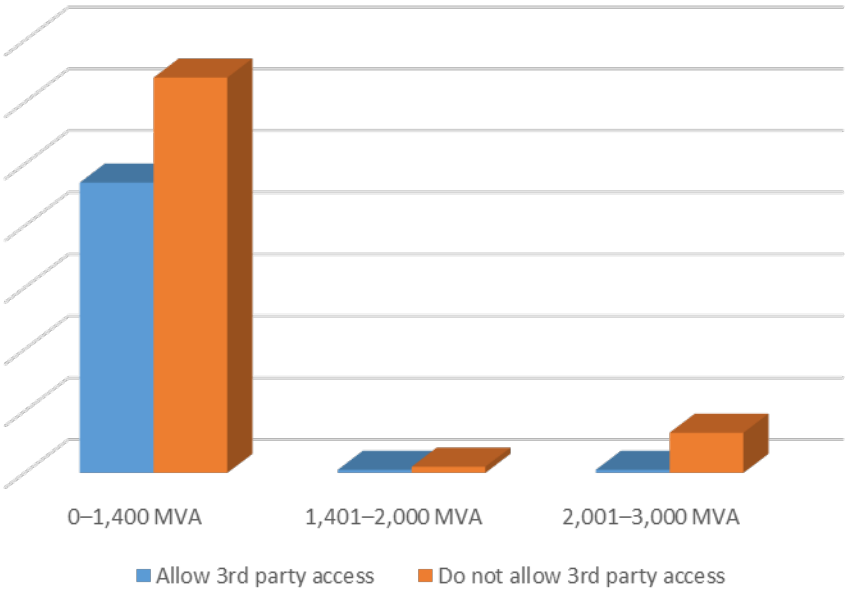


Figure 2.7: Transmission Stations and Substations for Entities with only Low Impact BES Cyber Systems

Likewise, NERC examined the data to determine whether third-party access was allowed at generation resource locations with low impact BES Cyber Systems. **Figure 2.8** shows the data for generation resources for entities that have a combination of low, medium, and high impact BES Cyber Systems. More of these generation locations, with less than 500 MW, allow third-party access than do not. **Figure 2.9** shows the data for generation resources for entities that have only low impact BES Cyber Systems. A significant percentage of these locations allow third-party access. In addition, while no values are presented in this report, the total number of locations represented in **Figure 2.9** represents 23% of all generation resource locations reported with low impact BES Cyber Systems. This is a significantly higher percentage than that represented by transmission stations and substations. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly affect BES reliability beyond the local area.

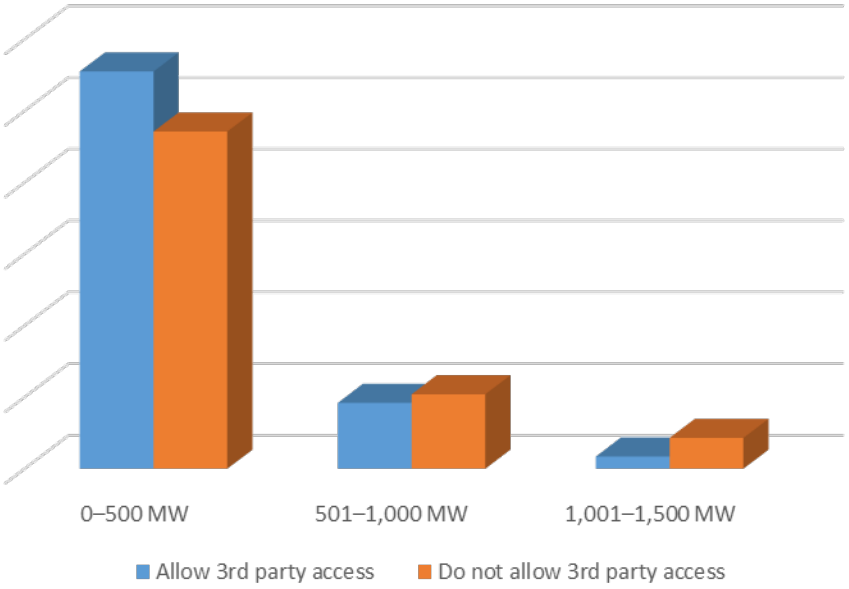


Figure 2.8: Generation Resources for Entities with High, Medium, and Low Impact BES Cyber Systems

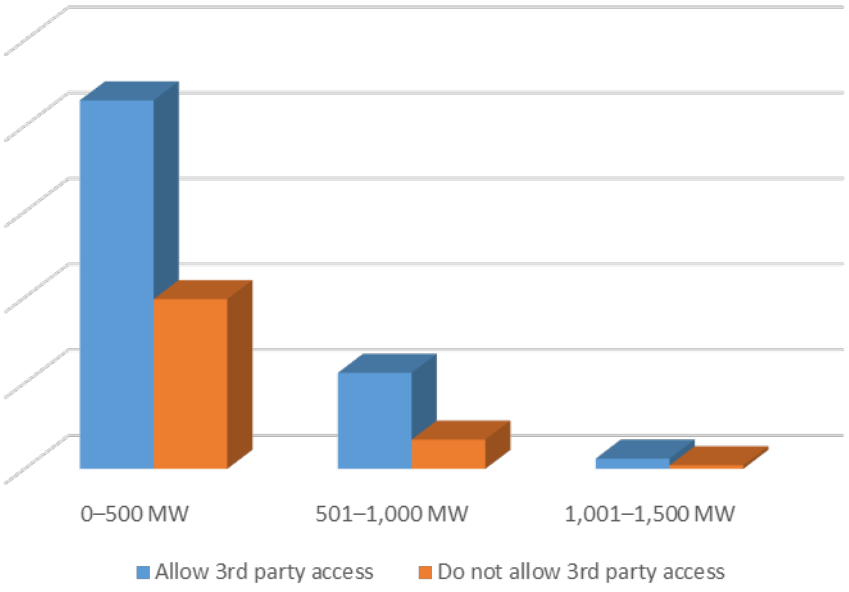


Figure 2.9: Generation Resources for Entities with only Low Impact BES Cyber Systems

Chapter 3: Conclusion

Supply chain compromise of industrial control system hardware, software, and computing and networking services associated with BES operations could pose a threat to BES reliability. The Supply Chain Standards require responsible entities that possess high and medium impact BES Cyber Systems to develop processes to manage supply chain risks through the procurement process. The Supply Chain Standards as currently approved apply to the higher-risk systems that have the greatest impact to the grid.

Based on the analysis of the data and in consideration of the common device supply chain risk, NERC staff recommends the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

When assessing the data, NERC staff made a few observations. First, most low impact assets reside in organizations with higher impact assets that are applicable to the approved Supply Chain Standards. The analysis of the data is contrary to the expectation in the Supply Chain Study that entities possessing medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. Namely, when asked in the survey how their CIP-013-1 R1 plan will affect their low impact BES Cyber Systems (Question 4 of the data request), entities provided inconsistent responses. Some stated that they plan to use a documented enterprise-wide Supply Chain Cyber Security Risk Management plan that includes all BES Cyber Systems (high/medium/low). Others stated that they do not intend to apply their supply chain risk management plans to their low impact BES Cyber Systems, especially involving vendors that were not supplying high or medium impact BES Cyber Assets.

Another observation was that most low impact BES Cyber Asset locations are individually lower risk based on the location risk score table in the survey. The vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have only one line greater than 300 kV at most or two lines greater than 200 kV but less than 300 kV. Similarly, the vast majority of generation resource low impact BES Cyber Assets are at locations that have less than 500 MW. An individual compromise to any one of these locations (transmission station and substation or generation resource) would generally be a localized event. However, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection-wide BES reliability impact.

One method to counter a coordinated cyberattack is to limit or eliminate third-party electronic access to locations. NERC observed entities that have a combination of low, medium, and high impact BES Cyber Systems in transmission stations and substations generally do not allow third-party access. However, entities that have only low impact BES Cyber Systems mostly allow third-party access to a significant number of their transmission stations and substations. As noted in **Chapter 2**, these locations represent only 3% of all transmission stations and substation locations reported with low impact BES Cyber Systems. That said, the combined effect of a coordinated cyberattack at multiple locations could impact BES reliability beyond their local area; this is an area of concern.

The analysis of third-party electronic access to generation resource locations is even more concerning. More than 50% of all generation resource locations allow third-party electronic access, whether entities have only low impact BES Cyber Systems or a combination of low, medium, and high impact BES Cyber Systems. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly impact BES reliability beyond the local area.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-9

October 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

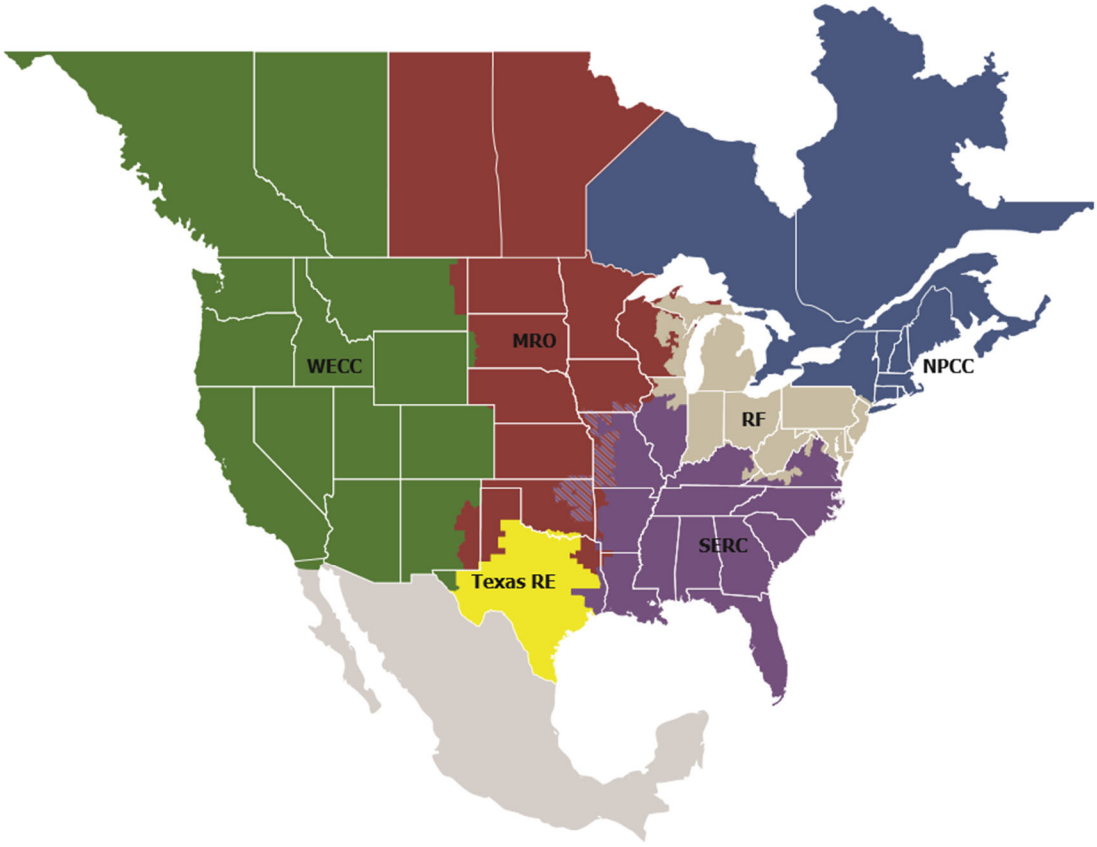
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-9

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

[1] Supply Chain Risk Assessment Report (nerc.com)
[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and

[3] CIP-013 Technical Rationale

maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G

Summary of Development History and Complete Record of Development

Summary of Development History

The following is a summary of the development record for proposed Reliability Standard CIP-003-9.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team ("SDT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the SDT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2020-03 SDT members is included in **Exhibit H**.

II. Standard Development History

A. Board of Trustees Action

At its May 9, 2019 meeting, the NERC Board of Trustees accepted the Staff Report, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, which recommended data collection to determine the need for Reliability Standards revisions.[3] After collecting and analyzing the data, NERC staff published the *Supply Chain Risk Assessment* report= in December, 2019 that included recommendations to develop Reliability Standards requirements for supply chain risk management for low impact BES Cyber Systems.[4] At its February 6, 2020 meeting, the Board

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2018).

2 The NERC *Standard Processes Manual* is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

3 NERC Board of Trustees May 9, 2019 Meeting Minutes at 11, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_Final_Minutes-May-9-2019.pdf.

4 NERC, *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request*, available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf.

approved NERC staff's recommendation to initiate a project to modify Reliability Standard CIP-003-8 to include low impact Bulk Electric System ("BES") Cyber Systems with remote electronic access connectivity.[5]

B. Standard Authorization Request Development

On March 18, 2020, the Standards Committee authorized posting a Standards Authorization Request ("SAR") developed in response to the *Supply Chain Risk Assessment* report for an extended informal comment period from April 03, 2020 through June 3, 2020 and authorized the solicitation of SDT members.[6] On July 22, 2020 the Standards Committee appointed the Project 2020-03 Supply Chain Low Impact Revisions SAR Drafting Team DT and authorized the solicitation of additional members.[7] On November 19, 2020, the Standards Committee appointed two additional members to the SAR DT.[8] The Standards Committee accepted the revised SAR on February 17, 2021.[9]

C. First Posting - Comment Period, Initial Ballot, and Non-binding Poll

On June 25, 2021, the Standards Committee authorized initial posting of proposed Reliability Standard CIP-003-9, the associated Implementation Plan and other associated

---

5 NERC Board of Trustees, *Minutes* at p. 13, https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf.

6 *See* NERC Standards Committee March 18, 2020 Agenda Package, Agenda Item 8. https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20Agenda%20Package_March2020.pdf.

7 *See* NERC Standards Committee July 22, 2020 Agenda Package, Agenda Item 5. https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_July_22_2020.pdf.

8 *See* NERC Standards Committee November 19, 2020 Agenda Package, Agenda Item 6. https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_November_19_2020.pdf.

9 *See* NERC Standards Committee February 17, 2021 Agenda Package, Agenda Item 4. https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_February_17_2021.pdf.

documents for a 45-day formal comment period.[10] The initial posting took place from August 27, 2021 through October 11, 2021, with a parallel ballot and non-binding poll on the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") held during the last 10 days of the comment period from October 1, 2021 through October 11, 2021. The initial ballot for proposed Reliability Standard CIP-003-9 received 29.2 percent approval, reaching quorum at 83.22 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 28.65 percent supportive opinions, reaching quorum at 83.45 percent of the ballot pool.[11] There were 82 sets of responses, including comments from approximately 192 different individuals and approximately 128 companies, representing all 10 industry segments.[12]

D. Second Posting - Comment Period, Additional Ballot, and Non-binding Poll

Proposed Reliability Standard CIP-003-9, the associated Implementation Plan and other associated documents were posted for a 45-day formal comment period from February 25, 2022 through April 15, 2022, with a parallel additional ballot and non-binding poll held during the last 10 days of the comment period from April 6, 2022 through April 15, 2022.[13] The additional ballot for the proposed Reliability Standard CIP-003-9 received 52.62 percent approval, reaching quorum at 81.44 percent of the ballot pool.[14] The non-binding poll for the associated VRFs and VSLs received 49.43 percent supportive opinions, reaching quorum at 81.95 percent of the ballot pool.[15] There were 75 sets of responses, including comments from approximately 167 different individuals and approximately 114 companies, representing all 10 industry segments.[16]

---

[10] *See* NERC Standards Committee June 25, 2021 SCEC Action without a Meeting, Agenda Item 1. https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SCEC%20Action%20without%20a%20Meeting%20-%20June%2025,%202021.pdf.

[11] *See* Exhibit F, Complete Record of Development, at items 23, 24.

[12] *Id.* at items 19, 20.

[13] *Id.* at item 37.

[14] *Id*. at item 38.

[15] *Id*. at item 39.

[16] *Id.* at items 34, 35.

E. Third Posting - Comment Period, Additional Ballot, and Non-binding Poll

Proposed Reliability Standard CIP-003-9, the associated Implementation Plan and other associated documents were posted for a 45-day formal comment period from July 6, 2022 through August 19, 2022, with a parallel additional ballot and non-binding poll held during the last 10 days of the comment period from August 10, 2022 through August 19, 2022.[17] The additional ballot for the proposed Reliability Standard CIP-003-9 received 66.81 percent approval, reaching quorum at 85.22 percent of the ballot pool.[18] The non-binding poll for the associated VRFs and VSLs received 67.84 percent supportive opinions, reaching quorum at 84.12 percent of the ballot pool.[19] There were 75 sets of responses, including comments from approximately 175 different individuals and approximately 105 companies, representing all 10 industry segments.[20]

F. Final Ballot

Proposed Reliability Standard CIP-003-9 was posted for a 10-day final ballot period from October 26, 2022 through November 4, 2022.[21] The ballot for proposed Reliability Standard CIP-003-9 and associated documents reached quorum at 86.25 percent of the ballot pool, receiving support from 68.95 percent of the voters.[22]

G. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standard CIP-003-9 on November, 16 2022.[23]

---

17 *Id*. at item 51.
18 *Id*. at item 53.
19 *Id*. at item 54.
20 *Id*. at items 49, 50.
21 *Id.* at item 64.
22 *Id*. at item 65.
23 NERC, *Board of Trustees Agenda Package November 16, 2022*, Agenda Item 6a. (Project 2020-03 Supply Chain Low Impact Revisions), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Meeting_November_16_2022_Agenda_Package_ATTENDEEv2.pdf.

Complete Record of Development

Project 2020-03 Supply Chain Low Impact Revisions

Related Files

Status

The final ballot for **CIP-003-9 - Cyber Security — Security Management Controls** concluded **8 p.m. Eastern, Friday, November 4,** 2022. The voting results can be accessed via the link below. The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) have both made modifications to CIP-003. In previous postings, the Supply Chain team is used"-X" in place of the version number, and Virtualization used "-Y". In preparation for the filing with the NERC Board of Trustees, Supply Chain has updated the version number to CIP-003-9.

Background

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Standard(s) Affected – CIP-003-8

Purpose/Industry Need

This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Subscribe to this project's observer distribution list

Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2020-03 Supply Chain Low Impact Revisions Observer List" in the Description Box.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft **(55)** Clean | **(56)** Redline to Last Posted | **(57)** Redline to Last Approved Implementation Plan **(58)** Clean | **(59)** Redline **Supporting Materials** Technical Rationale **(60)** Clean | **(61)** Redline **(62)** VRF/VSL Justifications **(63)** Reliability Standard Audit Worksheet (RSAW)	Final Ballot **(64)** Info Vote	10/26/22 - 11/04/22	**(65)** Ballot Results	
Draft 3 CIP-003-X **(40)** Clean | **(41)** Redline Implementation Plan **(42)** Clean | **(43)** Redline	Additional Ballot and Non-binding Poll **(51)** Updated Info **(52)** Info Vote	08/10/22 – 08/19/22	**(53)** Ballot Results **(54)** Non-binding Poll Results	
Supporting Materials **(44)** Unofficial Comment Form (Word) Technical Rationale **(45)** Clean | **(46)** Redline **(47)** VRF/VSL Justifications	Comment Period **(48)** Info Submit Comments	07/06/22 – 08/19/22	**(49)** Comments Received	**(50)** Consideration of Comments
Draft 2 CIP-003-X **(25)** Clean | **(26)** Redline Implementation Plan **(27)** Clean | **(28)** Redline	Additional Ballot and Non-binding Poll **(36)** Updated Info (Ballot Open Reminder) **(37)** Info(Updated) Vote	04/06/22 - 04/15/22 (Updated prevent projects closing on the same days)	**(38)** Ballot Results **(39)** Non-binding Poll Results	
Supporting Materials **(29)** Unofficial Comment Form (Word)	Comment Period	02/25/22 - 04/15/22		

Technical Rationale **(30)** Clean | **(31)** Redline **(32)** VRF/VSL Justifications	**(33)** Info (Updated) Submit Comments	(Updated to prevent projects closing on the same days)	**(34)** Comments Received	**(35)** Consideration of Comments
Draft 1 CIP-003-X **(12)** Clean | **(13)** Redline **(14)** Implementation Plan **Supporting Materials** **(15** Unofficial Comment Form (Word) **(16)** VRF and VSL Justifications **(17)** Technical Rationale	Initial Ballot and Non-binding Poll **(21)** Updated Info **(22)** Info Vote	10/01/21- 10/11/21	**(23)** Ballot Results **(24)** Non-binding Poll Results	
	Join Ballot Pools	08/27/21 - 09/27/21		
	Comment Period **(18)** Info Submit Comments	08/27/21- 10/11/21	**(19)** Comments Received	**(20)** Consideration of Comments
Standard Authorization Request (SAR) **(10)** Clean | **(11)** Redline	The Standards Committee accepted the SAR on February 17, 2021			
Supplemental Drafting Team Nominations **(8)** Unofficial Nomination Form (Word)	Nomination Period **(9)** Info Submit Nominations	07/30/20 - 08/13/20		
(3) Standard Authorization Request **Supporting Materials** **(4)** Unofficial Comment Form (Word)	Comment Period **(5)**Info (Updated) Submit Comments	04/03/20 - 06/03/20 (Extended)	**(6)** Comments Received	**(7)** Summary Response to Comments
Drafting Team Nominations **Supporting Materials** **(1)** Unofficial Nomination Form (Word)	Nomination Period **(2)** Info (Updated) Submit Nominations	04/03/20 - 06/03/20 (Extended)		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2020-03 Supply Chain Low Impact Revisions** drafting team members by **8 p.m. Eastern, Wednesday, June 3, 2020.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information about this project is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Supply Chain Low Impact Revisions

In adopting the Supply Chain Standards in August 2017, the NERC Board concurrently adopted additional resolutions related to implementation and risk evaluation. These resolutions included preparation of a study of cyber security supply chain risks. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018. In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks.[1] NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or

[1] *See* NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 17, 2019). This report, and the other materials referenced in this item, are available on NERC's Supply Chain Risk Mitigation Program page at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Standards affected: CIP-003-8

The time commitment for these projects is expected to be up to two face-to-face meetings per quarter (on average two and a half full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome. NERC is seeking individuals who have significiant subject matter expertise with the Critical Infrastructure Protection ("CIP) family of Reliability Standards and Cyber Asset and BES Cyber Asset definitions. Expertise with of remote access or network design is needed.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	
Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):	
If you are currently a member of any NERC drafting team, please list each team here: ☐ Not currently on any active SAR or standard drafting team. ☐ Currently a member of the following SAR or standard drafting team(s):	
If you previously worked on any NERC drafting team please identify the team(s): ☐ No prior NERC SAR or standard drafting team. ☐ Prior experience on the following team(s):	

Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.
☐ Yes, the nominee has read and understands these documents.

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:		
☐ MRO ☐ NPCC ☐ RF	☐ SERC ☐ Texas RE ☐ WECC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[2] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

[2] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions

Nomination Period Now Open through June 3, 2020

Now Available

Nominations are being sought for **Project 2020-03 Supply Chain Low Impact Revisions** drafting team members. The due date has been extended, and is now open through **8 p.m. Eastern, Wednesday, June 3, 2020**.

Use the electronic form to submit a nomination. Contact Wendy Muller regarding issues using the electronic form. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls. Previous drafting team experience is beneficial but not required.

See the project page (linked above) and nomination form for additional information.

Next Steps
The Standards Committee is expected to appoint members to the drafting team in June or July 2020. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security		
Date Submitted:	March 4, 2020		
SAR Requester			
Name:	Soo Jin Kim, Senior Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The project will increase reliability through consistent supply chain protections to low impact BES Cyber Systems. The NERC Supply Chain Risk Assessment Report (December 2019) found that 87% of all BES Cyber Asset locations have low impact BES Cyber Systems, and many of these locations have external connectivity. Currently the systems at these locations would not be subject to the current Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. The impact to the reliability of the BES could be significant if multiple owners and operators allow third-party access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect

Requested information
known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Project Scope (Define the parameters of the proposed project):
This project will address recommendations form the NERC Supply Chain Risk Assessment Report. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to definition or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Revise CIP-003-8 to include policies for low impact BES Cyber Systems at locations that allow 3rd party remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions, standards or requirements.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **Project 2020-03 Supply Chain Low Impact Revisions Standard Authorization Request (SAR).** Comments must be submitted by **8 p.m. Eastern, Wednesday, June 3, 2020.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

On July 21, 2016, FERC issued Order No. 829, directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system (BES) operations. Following the issuance of this order, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-005-6 and CIP-010-3.

In adopting the Supply Chain Standards in August 2017, the NERC Board concurrently adopted additional resolutions related to implementation and risk evaluation. These resolutions included preparation of a study of cyber security supply chain risks. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018. In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks.[1] NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

[1] *See* NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 17, 2019). This report, and the other materials referenced in this item, are available on NERC's Supply Chain Risk Mitigation Program page at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

2. Provide any additional comments for the SAR drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions
Standard Authorization Request

Informal Comment Period Now Open through June 3, 2020

Now Available

The informal comment period for the **Project 2020-03 Supply Chain Low Impact Revisions Standard Authorization Request** *has been extended and is now open through* ***8 p.m. Eastern, Wednesday, June 3, 2020.***

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues with the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project**.**

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions | Standard Authorization Request
Comment Period Start Date:	4/3/2020
Comment Period End Date:	6/3/2020
Associated Ballots:	

There were 49 sets of responses, including comments from approximately 106 different people from approximately 84 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Robert Rhett	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO

					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
Westar Energy	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Scott Brame	North Carolina EMC	3,4,5	SERC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF

					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Northern California Power Agency	Marty Hostler	3,4,5,6		NCPA	Michael Whitney	Northern California Power Agency	3	WECC
					Scott Tomashefsky	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
					Marty	Northern California Power Agen	5	WECC
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC

Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	No
Document Name	

Comment

Some smaller agencies rely soely on thrid parties to proved all of the cyber services because they do not have a Information Technology department or staff. Extending the proposed requirments down to smaller utilities, such as monitoring remote access, will have a significant burden on these utilities. They will not have the resources to manage a standard like this.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Detection of "known or suspicious malicious communications" should only apply to "active vendor remote access sessions." That is, normal data communications between BES Cyber Systems inside the asset and cyber systems outside should not be part of the scope of this proposal as they have nothing to do with the supply chain. This may be what is intended in this proposal but it is not clearly stated.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

Extending the proposed requirements to low impact facilities will have a significant financial and resource management burden on utilities.

Likes 0	

Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

- These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments".

The NSRF agrees this SAR is for policy inputs for low impact BES Cyber Systems that allow 3rd party vendor remote access. The first point to be contained in a policy is unclear.

"(1) detect known or suspected malicious communications for both inbound and outbound communications". We don't know what "malicious communication" is meaning within this first attribute? The Supply Chain Risk Assessment Report (linked within the SAR) only uses "malicious", twice. Once in the Background section and once in foot note 15. Both instances do not describe what "malicious communication" is or how it could be applied. Without a clear understanding of what the intent of "malicious communications" is, the Standard Drafting Team may not satisfy the intent of the NERC BOT and the Supply Chain Risk Assessment Report. Does "malicious" cover every type of act that could do harm? From physical to cyber (DOS, Phishing, malware, social engineering, cutting communication cables, etc.)?

We also question why the first attribute wants the detection of "known and suspected" since both are considered malicious. Recommend that "known and suspected" be deleted and it will now read "(1) detect malicious …".

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No
Document Name	

Comment

N&ST recommends against the proposed modification of CIP-003-8 to include policies for low impact BES Cyber Systems to detect known or suspected malicious communications for both inbound and outbound communications (Item 1, above), for the following reasons:

- At the present time this requirement, as established by CIP-005-6 R1 Part 1.5, applies only to High and Medium impact BES Cyber Systems at Control Centers. Adding a similar requirement to CIP-003-8 would result in some assets with Low Impact BES Cyber Systems being subject to more stringent communication security requirements than apply to Medium Impact BES Cyber Systems with External Routable Connectivity at BES assets other than Control Centers.

- There is no explicit statement of concern about "known or suspected malicious communications" in the NERC Supply Chain Risk Assessment final report.

- As written, the SAR could lead to a “malicious communication detection” requirement for Low Impact assets with BES Cyber Systems REGARDLESS of whether or not they allow “vendor remote access.”

N&ST also recommends modifying the SAR to address the following concerns:

- It should be clear that new requirements for “vendor remote access” will apply only to those BES assets that (1) contain Low Impact BES Cyber Systems and (2) are subject to the existing electronic access control requirements in CIP-003-8 Attachment 1, Section 3.

- Any and all supply chain - related terms introduced in a revised version of CIP-003 should be consistent with terms already used in CIP-005-6. N&ST noted the SAR refers to both “vendor remote access,” which appears in CIP-005-6, and “3rd party remote access,” which does not appear in CIP-005-6. N&ST strongly believes the latter phrase should not be used, as it would likely sow confusion about requirement applicability.

- Regarding the draft SAR’s statement about potential costs, “Cost impact is unknown at this time,” N&ST believes that new requirements to detect and manage “vendor remote access” may, for some entities, require a complete overhaul of their existing Low Impact electronic access control implementations, significant investments in new networking equipment, or both.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF is in agreement with the three items in the proposed scope for this SAR, but we think the scope should include mitigation for supply chain cyber security risk for low impact. This could include in current Supply Chain Cyber Security Risk Management plan for high and medium impact BES Cyber Systems or something just for low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

In the Industry Need, request replace “third party” with “vendor” for consistency with the rest of this SAR.

In the Goals section, we disagree with the inclusion of Goal #1 in the SAR, to “detect known or suspected malicious communications for both inbound and outbound communications” for the following reasons:

1) This provision is not included as a recommendation in the “NERC Supply Chain Risk Assessment Report (December 2019).”

2) The CIP-005, requirement that aligns with this goal is for Control Centers only.

3) The current wording of this goal would apply to all communications and not just those paths used for vendor remote access or even just those that use ERC.

Applying Goal 1 to low impact facilities is inconsistent with the stated purpose of the SAR and overly burdensome on low impact Facilities.

CIP-005 allows for TFEs for the medium and high impact requirements that align with Goals #2 and #3. Consideration should be given to the handling of TFEs at low impact Facilities. With the number of low impact Facilities that are going to apply these requirements, using the TFE process would be overly burdensome and not provide a significant benefit to reliability.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree with the proposed scope as described in the SAR. Duke Energy supports the overall intent to modify CIP-003-8 to include policies for mitigating risks posed by third party electronic access to low impact BES Cyber Systems or Assets containing those systems.

Duke Energy recommends clarification of the project scope and purpose to move forward with an approach that characterizes the risks to the BES, as a whole, posed by 3rd party access to low impact BES Cyber Systems or Assets containing those systems. Duke Energy recommends such a risk characterization be employed to provide an appropriate risk informed mitigation. The detailed description as written implies a solution that may impose significant burden on owners with existing system architectures which may not support the required modifications, or be may not be commensurate with the actual risk.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC believes the scope as written is too broad and ccould be written to better align with the intent of the SAR.

Potential suggestions would be:

(2) implement methods to monitor for and detect known or suspected vendor-initiated malicious communications for both inbound and outbound communications;

(1) implement methods to determine when active vendor remote access sessions are initiated; and

(3) disable active vendor remote access when necessary.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Although the CAISO acknowledges that low impact BES Cyber Systems with remote electronic access connectivity are important to protect in line with the FERC Order, we recommend to wait on extending the program to them until after the upcoming CIP-005-6, CIP-010-3 and CIP-013-1 standards have been in effect for at least two years to allow for the processes and controls to mature and to obtain any key learnings from implementing these protections and from audit experiences, including findings and areas of concerns identified by the auditors. At that time, the CAISO also proposes that NERC issue a CIP-013-1 survey amongst the industry to collect recommendations for improvement of the industry's supply chain security standard.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The proposed SAR for CIP-003 changes are specific to electronic access controls for vendor remote access, but the SAR does not address introduced and increased risk of supply chain procurements of low impact BES Cyber Systems. Vendors remotely accessing sites/assets and the associated low impact BES Cyber Systems present a substantial risk, but the proposed new requirements do not address vulnerabilities vendors may introduce to low impact BCS, ranging from potential compromised access, revocation of vendor access, no awareness of vendor incidents, no disclosure of known vulnerabilities related to products used with low impact BCS, etc. For example, entities without awareness of a vendor's vulnerabilities or coordination of responses to incidents could impact countless low impact BCS across several registered entities throughout Interconnections.

NERC's December 2019 report affirms a coordinated attack across low impact BES Cyber Systems could introduce significant adverse impact on reliability. Simply defining access controls for vendors does not mitigate other notable risks introduced with the supply chain of products and services supporting low impact BCS. For low impact sites/assets, several vendors are used for maintenance and operation functions and responsibilities. The absence of a proper risk assessment of vendor services and/or products for low impact BES Cyber Systems could potentially have an adverse impact to the BES. The SAR should be revised to ensure inclusion of low impact BCS with supply chain risk management.

Further, with the recent publication of the Executive Order Number 13920, the SAR should be expanded to include supply chain risk management with low impact BES Cyber Systems. It is a growing risk and initiating forward momentum in Project 2020 03 could assure alignment of the ERO with all impacted bulk power industries, not just those affiliated with NERC.

Likes 0	
Dislikes 0	
Response	

Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Evergy (Westar Energy and Kansas City Power & Light), incorporate by reference and support the Edison Electric Institute (EEI) response to Question 1.

Likes 0	
Dislikes 0	
Response	

Tony Skourtas - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	

The policy to detect malicious communications will be a significant increase in user action for the low-impact category and is in contrast to the nominal NERC CIP approach, which uses an asset-centric, risk-based method. As the NERC Report indicated, the risk based scores from the survey data are low.

This Standard revision is occurring as part of the supply chain risk management efforts, but it seems like the scope exceeds vendor remote access to low-impact BES assets. Further clarification on applicability is needed.

Likes 0	
Dislikes 0	
Response	

Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	

AEP does not agree with the scope of the proposed SAR as written, as it currently appears to use the terms “vendor” and “3rd party” interchangeably. Indeed, the Supply Chain Risk Assessment also appears to use these terms as one in the same, which likely resulted in the “Goal and Purpose” of the SAR referring to **vendor** access, while the “Detailed Description” refers to locations with **3rd party** remote access.

As such, the proposed SAR is unclear in it stated purpose. AEP believes that should this project move forward, that the terms “vendor” and “3rd party” would need to be formally defined, and that work should take place either prior to, or in conjunction with, this project. This will provide the industry the clarity needed to fully understand and implement any requirement(s) developed in the revised Standard.

As reference, a “vendor” is typically an independent entity that provides a service or product, and may or may not be vetted for their security posture. While a “3rd party” can be a person or entity that is a contractor for a registered entity that performs certain duties, and has been vetted with the same scrutiny as employees, or even a neighboring utility employee that has the need to access information from a common facility.

It also worth noting that FERC Order 829, which directed NERC to develop the Supply Chain Standards, refers to mitigating vendor risk, specifically it states:

“[FERC directs] “*NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2)* ***vendor*** *remote access; (3) information system planning; and (4)* ***vendor*** *risk management and procurement controls.”*

Likes 0	

Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

The Project 2020-03 on Supply Chain Low Impact Revisions will continue to distort the primary goal of the NERC CIP-003 Standard, which is Security Management Controls. Most of the requirements in this standard are about “Management”. By continuing to address Low Impact BES Cyber Systems (L-BCS) within the CIP-003, we distort the standard.

Requirements 1, 3 and 4 of CIP-003 are about real management concerns: what is subject to CIP Senior Manager’s approval, the identification of a CIP Senior Manager and its authority delegation. R2 of CIP-003 is about L-BCS and don’t have its place into CIP-003.

As we are going to address L-BCS almost like M-BCS or H-BCS, we should address L-BCS like High and Medium BCS. We should status if a given requirement is applicable to Low (L-BCS). If yes, add it in the “Applicable Systems” column of the given requirement. I don’t understand why we have to make an exception of L-BCS.

The new requirement “(1) detect known or suspected malicious communications for both inbound and outbound communications” for Electronic Access Points (EAP) for L-BCS already exists as R1.5 in CIP-005 standard for EAP of M-BCS at control centers and EAP of H-BCS. Doing this is a non-sense if we apply the requirement to all EAP for L-BCS without applying that requirement to all EAP for M-BCS.

The new requirement “(2) determine when active vendor remote access sessions are initiated” is almost similar to R1.3 (and R1.4 maybe) in CIP-005 standard on EAP for M-BCS and H-BCS.

The new requirement “(3) disable active vendor remote access when necessary” is similar to a part of R1.3 in CIP-005 standard on EAP for M-BCS and H-BCS: “… deny all other access by default”. At least, it could be a new requirement of CIP-005 standard, dedicated to EAP for L-BCS.

With the Transient Cyber Asset (TCA) used on L-BCS: because CIP-010 is covering TCA used on M-BCS, why didn’t we group together TCA used on L-BCS? WE should keep the concerns of the same nature all together. Many times, TCA used on M-BCS will be used or could be also used on some L-BCS. Using CIP-003 to cover TCA used on L-BCS and CIP-010 to cover TCA used on M-BCS is a non-sense.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - NAGF - 6 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

NAGF Comments:

We agree with need to address the risk to the grid from low-impact remote access and therefore with the intent of the SAR. However, the requirements that could come out of the SAR, the way that it is currently written could result in low-impact generation entities facing stricter requirements than medium-impact generation entities. In addition, the requirements that could result from the SAR, as it is currently written, could be a significant cost to organizations requiring retrofit of existing systems and could require contract negotiations with vendors. To address these, and other concerns, we would like to see the following considered in a revised SAR and/or in the draft standard itself:

1. **SAR Scope & Detailed Description**:

The "Project Scope" section of the SAR does not set a clear enough scope for the project. This section should be modified to direct the creation of a standard or revision of a standard to address the security objective of mitigating the risk posed by vendor/3rd party remote access to assets containing low impact BES Cyber Systems while still allowing the entity flexibility in how to meet these objectives.

Consistent with the wording used in the CIP-002 (and CIP-003) standards the "**Detailed Description**" section be modified from "low impact BES Cyber Systems at locations" to "assets containing low impact BES Cyber Systems". Concerns with the specific security requirements (1-3) included in the Detailed Description section have been outlined below. It is also noted that this section switches terms from "vendor" to "3rd party", this should be corrected to be consistent and defined.

2. Diversity of Bulk Electric System low impact entities:

The SAR should be written in a manner that will result in a standard that does not impose ''one-size fits all'' language. Within the low-impact category there are significant differences that exist among entities and this standard must be flexible enough to account for the differences in the needs and characteristics of responsible entities, the diversity of the Bulk Electric System environments, technologies, risks and issues related to the limited applicability of mandatory NERC reliability standards. In keeping with FERC Order No. 829, the SAR should accommodate different controls based on the criticality of different assets. This flexibility in the 2016-03 SAR allowed the SDT to apply the requirement for medium and high impact entities to detect malicious communication both inbound and outbound (CIP-005-5 R1.5) at varying degrees depending on risk to the grid.

- **Security Requirement 1: Detect known or suspected malicious communications for both inbound and outbound communications**

A similar requirement exists under CIP-005-5 R1.5 for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers. Imposing this regulation on low impact BES Cyber Systems before it is imposed on the entirety of medium impact cyber systems does not correlate with NERC's risk-based approach to compliance. This issue could be rectified if the SAR was amended to include more security objective language vs. specific security requirements as it does currently. As this security requirement is currently written it will require significant resources, rework / replacement of infrastructure recently installed and installation of new systems that are not required for higher risk medium impact generation registrations.

- **Security Requirement 2: Determine when active vendor remote access sessions are initiated**

For renewable sites that rely on OEM providers for ongoing maintenance and operational support, vendor remote access is required frequently. In some situations, especially where operational personnel are not on site 24/7 this vendor remote access is vital to ensuring that these largely dispersed, and often unmanned sites can actively support the reliability of the grid. We encourage the Standard Drafting Team to consider these situations and ensure the standard allows enough flexibility to accommodate.

We recommend that the SAR be revised to address the type of remote access that would be applicable to this requirement and expressly indicate if it is all remote access or is focused solely on Interactive Remote Access.

- **Security Requirement 3: Disable active vendor remote access when necessary**

We recommend that the Standard Drafting Team consider the physically remote locations of many low impact assets and the potential challenges applying this security requirement.

Likes 0	

Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	

Comment
San Miguel Electric Cooperative agrees with the comments submitted by Barry Lawson of NRECA. We agree with the intent to protect the Low - BCS from supply chain risks, but the SAR is written with detailed requirements that are not one-size fits all nor risk-based. Entities should evaluate the vulnerabilities/risks, and have flexibility on how to address them. The detailed requirements as written could result in Low-BCS requirements being more stringent than those for Medium-BCS. Entities should be required to evaluate risks and define needed controls. Any specific requirements should only apply to active vendor remote access that is not part of a normal or constant communication or monitoring service.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	

Comment
The language for (2) and (3) needs to match what was defined for CIP005-6 R2 Part 2.4 and Part 2.5. This ensures that the standards are consistent for High, Medium, and Low impact BCS that all External Routable Connectivity. Otherwise the language is vague and will lead to ineffective standards.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment

The proposed revisions bullet (1) “detect known or suspected malicious communications for both inbound and outbound communications” is directly borrowed from CIP-005-5 R1.5 for high and medium impact BCS, which has no direct linkage with bullet (2) & (3). If you want to link bullet (1), (2) and (3) together, we suggest changing the bullet (3) as follows:

“(3) disable active vendor remote access when the malicious communications are detected.”

The bullet (1) will bring a significant cost to industry for deploying IDS/IPS at low impact BCS sites with external routable connectivity. If this requirement is only based on a perception of an “aggregate misuse of numerous low impact BCS.”, we suggest developing a criterion to identify the aggregate points of low impact sites rather than applying this requirement to all low impact sites.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation (MRRE 80) - NA - Not Applicable - MRO,WECC,Texas RE,NPCC,SERC

Answer	No
Document Name	

Comment

We agree with need to address the risk to the grid from low-impact remote access and therefore with the intent of the SAR. However, the requirements that could come out of the SAR, the way that it is currently written could result in low-impact generation entities facing stricter requirements than medium-impact generation entities. In addition, the requirements that could result from the SAR, as it is currently written, could be a significant cost to organizations requiring retrofit of existing systems and could require contract negotiations with vendors. To address these, and other concerns, we would like to see the following considered in a revised SAR and/or in the draft standard itself

1. **SAR Scope & Detailed Description**:

The “Project Scope” section of the SAR does not set a clear enough scope for the project. This section should be modified to direct the creation of a standard or revision of a standard to address the security objective of mitigating the risk posed by vendor/3rd party remote access to low impact BES Cyber Systems while still allowing the entity flexibility in how to meet these objectives.

Consistent with the wording used in the CIP-002 (and CIP-003) standards the “**Detailed Description**” section be modified from “low impact BES Cyber Systems at locations” to “assets containing low impact BES Cyber Systems”. Concerns with the specific security requirements (1-3) included in the Detailed Description section have been outlined below. It is also noted that this section switches terms from “vendor” to “3rd party”, this should be corrected to be consistent and defined.

2. Diversity of Bulk Electric System low impact entities:

The SAR should be written in a manner that will result in a standard that does not impose ‘‘one-size fits all’’ language. Within the low-impact category there are significant differences that exist among entities and this standard must be flexible enough to account for the differences in the needs and characteristics of responsible entities, the diversity of the Bulk Electric System environments, technologies, risks and issues related to the limited applicability of mandatory NERC reliability standards. In keeping with FERC Order No. 829, the SAR should accommodate different controls based on the criticality of different assets. This flexibility in the 2016-03 SAR allowed the SDT to apply the requirement for medium and high impact entities to detect malicious communication both inbound and outbound (CIP-005-5 R1.5) at varying degrees depending on risk to the grid.

Security Requirement 1: Detect known or suspected malicious communications for both inbound and outbound communications

A similar requirement exists under CIP-005-5 R1.5 for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers. Imposing this regulation on low impact BES Cyber Systems before it is imposed on the entirety of medium impact cyber systems does not correlate with NERC's risk-based approach to compliance. This issue could be rectified if the SAR was amended to include more security objective language vs. specific security requirements as it does currently.

As this security requirement is currently written it will require significant resources, rework / replacement of infrastructure recently installed and installation of new systems that are not required for higher risk medium impact generation registrations.

Security Requirement 2: Determine when active vendor remote access sessions are initiated

For renewable sites that rely on OEM providers for ongoing maintenance and operational support, vendor remote access is required frequently. In some situations, especially where operational personnel are not on site 24/7 this vendor remote access is vital to ensuring that these largely dispersed, and often unmanned sites can actively support the reliability of the grid. We encourage the Standard Drafting Team to consider these situations and ensure the standard allows enough flexibility to accommodate.

We recommend that the SAR be revised to address the type of remote access that would be applicable to this requirement and expressly indicate if it is all remote access or is focused solely on Interactive Remote Access.

We recommend that if discrete security requirements such as this are incorporated into the standard, that the SDT try to ensure consistency in language, were possible, with other similar requirements (i.e. CIP-005-7 proposed language for R3 3.1: Have one or more methods for detecting vendor-initiated remote access sessions).

Security Requirement 3: Disable active vendor remote access when necessary

We recommend that the Standard Drafting Team consider the physically remote locations of many low impact assets related to any timeframe requirements associated with this requirement and the speed at which an entity may be able to disable vendor remote access.

We recommend that the standard add clarity regarding thresholds for determining the necessity of termination.

We recommend that if discrete security requirements such as this are incorporated into the standard, that the SDT try to ensure consistency in language, were possible, with other similar requirements (i.e. CIP-005-7 proposed language for R2 2.5 Have one or more method(s) to terminate established vendor-initiated remote access sessions).

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

Frist, Oncor suggests using "assets containing low impact BES Cyber System" rather than "low impact BES Cyber Systems at locations" in consistent with the current CIP-002 language.

Second, current requirement doesn't require to produce a list of low impact BES Cyber System. However, in order to fulfill the goals listed in the SAR, responsibility entity may have to create an inventory of low impact BES Cyber System and its associated software, hardware which would be difficult and over burden due to the high number of low impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
If these changes were accepted, this requirement would be more stringent than what is currently required for Medium Impact BCS and on par with the requirements for EAPs for Medium Impact Control Centers and High Impact BCS. We would not be in favor of elevating requirements for Medium Impact BCS in the future and are not in favor of this change for Low Impact BCS. Registered Entities (REs) recently completed their implementation of CIP-003-7 for Low Impact BCS. While the requirements in CIP-005 are best Cyber Security practices for Low Impact BCS, REs with only Low Impact BCS do not fall under CIP-005 compliance and do not always have systems, which would allow them to determine when active vendor remote access sessions are initiated (item #2) and disable active vendor remote access when necessary (item #3). This would require significant investment and management of remote access (if allowed by the RE), especially for small entities who are already resource-constrained. Further, Item #2 and Item #3 do not align with the Supply Chain Cyber Security risk management, but fall into the Electronic Access Controls area. These suggested changes do not enhance Supply Chain Cyber Security risk management for Low Impact BCS. Therefore, we do not see how these changes align with the scope of the background information provided for the scope of the SAR. The suggested requirements are purely Cyber Security related and do not pertain to Supply Chain Cyber Security risk management, nor the scope of the 1600 Data Request, and should be limited to the scope of FERC Order No. 829.	
Likes 0	

Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 3,4,5,6, Group Name NCPA

Answer	No
Document Name	

Comment

The following are technical reasons why NCPA does not support the subject SAR in its current form:

1. NERC's response to Market Principle 1 on SAR page 3 is inaccurate. CIP-003-8 will result in an unfair competitive advantage for non-GOPs in Regions that have BA/ISOs that don't allow GOPs to recover unfunded FERC mandated NERC compliance program fixed costs.

- California ISO (CAISO) Market rules, and maybe other ISOs too, do not allow GOPs to recover fixed costs for unfunded FERC/NERC reliability mandates. Non-GOP Market Participants have no said obligations nor costs.
- If this SAR is to move forward FERC needs to level the playing field and first order BAs to modify their Tariffs, and compensate GO/GOPs for fixed NERC Compliance Costs.
- Otherwise, at a minimum, this proposed Standard, among others, results in unfair Market competitive advantages for non-GOP generator Market Participants in the CAISO BA to the detriment, disadvantage of GOPs.
- This is an extremely unfair business practice especially considering the BAs/ISOs are compensated for, allowed to recover, 100% of their NERC/FERC fixed compliance costs.

2. NERC has not provided a cost estimate for this proposal. Future SARs should not be allowed though the Standards Committee without a cost estimate. All stakeholders need to know the estimated cost prior to SAR posting.

3. The President recently signed an Executive Order. The DOE is responsible for BES Supply Chain issues not FERC/NERC. Regardless, FERC, NERC, and Regional Entities still have not agreed how to enforce existing CIP-13 Standards that were to be effective July 1, 2020. In fact, they have ordered changes to CIP-005, 10, and 13, that no one can agree on either. Now they propose even more Supply Chain Standards.

If this SAR does move forward it should require the future CIP STD to not only develop standards, but develop guidance and audit approach measures, that Auditors shall be required to follow. And all of these need to be approved at the same time. No more, after-the-fact, Standards interruptions by FERC, NERC, and/or REs that were not approved by all Stakeholders.

4. We AGREE with Utility Services (Brian Evan Mongeon's) comments related to this SAR being inconsistent with prior stated goals, among other issues, which we will leave for others to discuss.

Likes 0	
Dislikes 0	

Response

Barry Jones - Western Area Power Administration - 9 - MRO,WECC

Answer	No

Document Name	

Comment

"(1) detect known or suspected malicious communications for both inbound and outbound communications". We don't know what "malicious communication" is meaning within this first attribute? The Supply Chain Risk Assessment Report (linked within the SAR) only uses "malicious", twice. Once in the Background section and once in foot note 15. Both instances do not describe what "malicious communication" is or how it could be applied. Without a clear understanding of what the intent of "malicious communications" is, the Standard Drafting Team may not satisfy the intent of the NERC BOT and the Supply Chain Risk Assessment Report. Does "malicious" cover every type of act that could do harm? From physical to cyber (DOS, Phishing, malware, social engineering, cutting communication cables, etc.)?

We also question why the first attribute wants the detection of "known and suspected" since both are considered malicious. Recommend that "known and suspected" be deleted and it will now read "(1) detect malicious …".

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6

Answer	No
Document Name	

Comment

WEC Energy Group concurs with and supports the EEI comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement should be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing malicious communications detection - "at locations that allow 3rd party remote access, have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications to low impact BES Cyber Systems where Cyber Asset(s), as specified by the Responsible Entity, provide electronic access control(s) implemented for Section 3.1."

(2) determine when active vendor remote access sessions are initiated;

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement could be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing vendor remote access – “at locations that allow 3rd party remote access, have one or more methods for determining active vendor remote access sessions” Purposefully leaving out the CIP-005-6 inclusion to keep things more generic.

From CIP-005-6 R2.4: *Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).*

(3) disable active vendor remote access when necessary.

This requirement could be addressed under the current CIP-003-8 Policy R1.2.3 Electronic access controls. The requirement could be specified under Attachment 1 Section 3, proposed here as a new part within Section 3 referencing vendor remote access – “at locations that allow 3rd party remote access, have one or more method(s) to disable active vendor remote access sessions” Purposefully leaving out the CIP-005-6 inclusion to keep things more generic.

From CIP-005-6 R2.5: *Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).*

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1 - MRO

Answer	No
Document Name	

Comment

MPC does not support the scope of the current project for the following reasons:

· The scope should be adjusted to include a definition for “vendor remote access”. Currently, this undefined term is open for interpretation. In some cases, the term’s interpretation brings web conferences into scope, even when a vendor does not have interactive access. Additionally, the term excludes other types of third parties that may provide remote support, such as a consultant. Also, if a vendor or other third party is onsite, is access via a jump host considered “vendor remote access”? The term “vendor remote access” should either be defined or replaced with a new, defined term, such as “third-party remote access” or “non-employee remote access”.

· MPC supports comments provided by Brian Evans-Mongeon, On Behalf of: Utility Services, Inc. · MPC supports comments provided by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports the proposed NERC Board of Trust (BOT) resolution that directs NERC to initiate a project to modify Reliability Standard CIP-003-8 to include specifically identified policies for low impact BES Cyber System, however, the following items need to be addressed in this SAR before we can support its approval: 1. EEI recommends that the SAR Scope be edited to align with the NERC BOT resolution which focuses on CIP-003-8. 2. EEI recommends that the text in the “Purpose or Goal” section be moved to the “Project Scope” section of the SAR. 3. The “Detailed Description” section appears to propose changes to the standard that would require an entity to create an inventory of low impact BES Cyber Systems and associated software to address the SAR. The existing standard has no obligation to create or produce such an inventory, and there does not appear to be a practicable way to implement the proposed supply chain processes without an inventory and associated inventory monitoring and update processes. Creating such an inventory of low impact BES Cyber Systems, which would be required to demonstrate compliance to the proposed standard, is overly burdensome and would not materially enhance reliability. EEI suggests that this section be revised so that it uses the currently approved wording in CIP-002 (and CIP-003) of “assets containing low impact BES Cyber Systems” rather than “low impact BES Cyber Systems at locations.” This keeps the SAR consistent with CIP-002 R1.3 which requires entities to “[i]dentify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).” EEI suggests changing this section to: Revise CIP-003-8 such that assets containing low impact BES Cyber Systems where the asset allows vendor remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.	
Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Tidwell Trevor
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	

Comment

IESO supports the comments submitted by NPCC

In the Industry Need, request replace “third party” with “vendor” for consistency with CIP-013.

In the Purpose / Goal, #1 is similar to CIP-005 Part 1.5 which is applicable to High / Medium Control Centers. Implementing Goal #1 would result in this requirement not applying to other Medium Impact assets while applying to High and Low. Next, we cannot find this concern as a recommendation in the study. So, we recommend removing Goal #1.

Goal #2 is similar to CIP-005 Part 2.4. Goal #3 is similar to CIP-005 Part 2.5. The corresponding Requirement 2 includes Technically Feasible Exception (TFE) language. If Goals #2 and #3 include TFE language, we do not believe the industry will achieve a desirable result. We recommend including a process for excluding communications based on capabilities without requiring a TFE.

CIP-005 Part 2.4 does not have the language “when initiated.” Recommend consistency with Part 2.4.

Project Scope says there are “recommendations” in the NERC Supply Chain Risk Assessment Report. That report makes only one recommendation. We request that the single recommendation be explicitly included in this Project Scope.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1,3,5 - NPCC

Answer	No
Document Name	

Comment

The Taunton Municipal Lighting Plant supports the comments submitted by Brian Evans-Mongeon of Utility Services, Inc., specifically the following:

In the Goals section, we disagree with the inclusion of Goal #1 in the SAR, to “detect known or suspected malicious communications for both inbound and outbound communications” for the following reasons:

1. This provision is not included as a recommendation in the “NERC Supply Chain Risk Assessment Report (December 2019).”
2. The CIP-005, requirement that aligns with this goal is for Control Centers only.
3. The current wording of this goal would apply to all communications and not just those paths used for vendor remote access or even just those that use ERC.

Applying Goal 1 to low impact facilities is inconsistent with the stated purpose of the SAR and overly burdensome on low impact Facilities.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	No
Document Name	
Comment	

NRECA has several significant and foundational concerns with the SAR and its scope as follows:

1. The proposed modifications are not technically justified or supported. The "NERC Supply Chain Risk Assessment Report (December 2019)" does not provide the necessary technical justification for the proposed scope of the SAR. The Cooperative Sector and NRECA provided detailed policy input to the NERC BOT for the February 2020 BOT meeting detailing our issues with the report's recommendation. This SAR appears to rely on that report for its technical justification and support, and, for that reason, NRECA respectfully re-asserts the following regarding its concerns about the justification for the proposed SAR:

a. The supply chain data request asked entities how their CIP-013-1, requirement R1 plan will affect low impact BES Cyber Systems and to describe the methods they intended to use to apply such plan to low impact BES Cyber Systems. This extremely narrowly-focused question did not allow for entities to provide any insight or guidance into other security-related procurement strategies that they may be employing during the procurement of low impact BES Cyber Systems, e.g., security-related contract provisions, third party risk reviews, chain of custody processes, etc. For those entities that have existing security-related procurement strategies that are NOT the result of or directly derived from the entity's specific CIP-013-1, requirement R1 plan, the response to this question would have been negative. However, such response also would not necessarily have been representative of an entity's security risk mitigation strategies for low impact BES Cyber System procurement. Accordingly, the responses gathered, and assumptions made regarding such responses are insufficient to support a determination that low impact BES Cyber Systems are not subject to security risk mitigation strategies during their procurement.

b. Using only the number of asset locations, NERC determined that a coordinated cyber-attack with control of multiple low impact locations could result in an event that has an interconnection-wide BES reliability impact. However, the actual potential for such an impact is closely correlated with the geographic and electrical location of assets within an interconnection, their individualized, aggregate ability for impact within and beyond their local area, the overall electrical configuration within which such issue would arise, and other essential factors and characteristics. Neither number nor any of these additional factors alone are determinative of the likelihood or risk of an aggregate, interconnection-wide reliability impact. Hence, without additional context and evaluation of the low impact assets and their associated low impact BES Cyber Systems, the determination that sheer numbers of locations (regardless of location, size, electrical impact, etc.) would aggregate into an interconnection-wide impact cannot be supported and should not form the basis for the modification of the scope or applicability of a reliability standard.

c. The generalized nature of the third-party access question also does not provide enough information and context for the true risk and potential for impact to be discerned. The risk of third-party access cannot be evaluated in isolation - without an understanding of any processes, controls, or risk mitigation strategies being employed when such access is granted. Given the right processes, controls, and risk mitigation strategies, granting a third-party access may not present any additional risk to the BES. For example, third party entities with access may be other registered electric industry entities with awareness of, and independent responsibility for, cyber security and reliability compliance. Additionally, an entity allowing third party access may have substantial and robust controls, such as background check requirements, continuous escorting, monitoring, or other protective measures. Further, while entities may allow third party access, criteria may be stringent; such access may be rare; and such access may have the effect of reducing risk and enhancing overall reliability. Without more information, there is not a true idea of actual risk to be addressed and mitigated.

d. Further, the current reliability standards for low impact BES Cyber Systems require that specific security controls be implemented to mitigate cyber security risk for these assets. It is unclear from the analysis provided whether NERC evaluated the effect of these required cyber security controls to determine their contribution to the mitigation of cyber security risk and the overall security of the BES.

For these reasons, NERC's finding of increased risk in its December 2019 report is premature and should not be relied upon as a basis for the modification of the scope or applicability of the reliability standards.

2. NRECA views the SAR as overly prescriptive by proposing specific technical requirements for inclusion in CIP-003-8. CIP-003-8 already prescribes a number of security controls be implemented for low impact assets. How or whether these current security controls contribute to or support the intent of these new specifications as well as how these new specifications get incorporated into reliability standards are typically within and should be within the purview of the expertise of the standards drafting team. NRECA posits that the proposed SAR should clearly identify and support a reliability objective/risk that needs to be addressed and not propose specific requirement language. The SAR should identify the risk (the what) and the SDT should evaluate the alternatives for requirement language (the how) to address such a risk.

3. The SAR states that no other alternatives have been considered for addressing the reliability objectives.

4. As proposed in the SAR, the new reliability standards requirements would result in low impact BES Cyber Systems being subjected to more stringent communication security requirements than medium impact BES Cyber Systems are generally. Currently, only medium impact BES Cyber Systems at Control Centers are subject to CIP-005-6, R1.5. This scope of assets was determined by the standards drafting team responsible for those requirements after much analysis and deliberate effort. Given this clear, deliberate scoping of BES Cyber Systems relative to CIP-005-6, R1.5, NRECA respectfully asserts that the current SAR represents a conflict with previous risk assessments. In particular, if medium impact BES Cyber Systems generally were not considered as a risk for malicious communication, the inclusion of low impact BES Cyber Systems does not seem justified or justifiable. NRECA requests that NERC re-evaluate this and remove this inappropriate requirement for low impact BES Cyber Systems.

In summary, NRECA requests that this proposed SAR should be remanded back to the requester to address the above comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNM Resources agree with EEI comments.
Additionally, to maintain consistency throughout the standards the Detailed Description, (2) and (3), should be aligned with the language ultimately used in CIP-005-7 R3.1 and R3.2, "Vendor Initiated Remote Access."

Likes 0	
Dislikes 0	

Response

Guy V. Zito - Northeast Power Coordinating Council - 10

Answer	No

Document Name	RS--5-5-20--2020-03_Supply_Chain_LIR_SAR_Unoffical_Comment_Form_04032020.docx
Comment	

In the Industry Need, request replace “third party” with “vendor” for consistency with CIP-013.

In the Purpose / Goal, #1 is similar to CIP-005 Part 1.5 which is applicable to High / Medium Control Centers. Implementing Goal #1 would result in this requirement not applying to other Medium Impact assets while applying to High and Low. Next, we cannot find this concern as a recommendation in the study. So, we recommend removing Goal #1.

Goal #2 is similar to CIP-005 Part 2.4. Goal #3 is similar to CIP-005 Part 2.5. The corresponding Requirement 2 includes Technically Feasible Exception (TFE) language. If Goals #2 and #3 include TFE language, we do not believe the industry will achieve a desirable result. We recommend including a process for excluding communications based on capabilities without requiring a TFE.

CIP-005 Part 2.4 does not have the language “when initiated.” Recommend consistency with Part 2.4.

Project Scope says there are “recommendations” in the NERC Supply Chain Risk Assessment Report. That report makes only one recommendation. We request that the single recommendation be explicitly included in this Project Scope.

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes

Document Name	

Comment

(1) detect known or suspected malicious communications for both inbound and outbound communications;

Southern supports the recommendation for the detection of known or suspected malicious communications for both inbound and outbound communications. However, the scope of the communication should be limited to routable communications. In addition, the scope of detection of malicious communications should be compatible with the CIP-003 access models.

(2) determine when active vendor remote access sessions are initiated; and

Southern supports this recommendation and requests that the SAR provide the SDT the flexibility to introduce new NERC defined terms, as needed, for Vendor Remote Access or alternatively, Low Impact Vendor Remote Access.

(3) disable active vendor remote access when necessary.

Southern supports this recommendation and, aside from the above comments, does not have any additional comments at this time.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Only where remote electronic access connectivity exists.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3,6	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Due to the high volume of assets containing low impact BES Cyber Systems and the need to review for compliance, we request the Implementation Period to be sufficient to support large organizations.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas agrees with adding certain policies for low impact BES Cyber Systems. Texas RE seeks clarification on whether CIP-013-1 will also be adjusted to include low impact BES Cyber Systems as an applicable system, in accordance with NERC's Supply Chain Risk Assessment. Texas RE recommends adding low impact BES Cyber Systems as an applicable system to CIP-013-1. Additionally, Texas RE recommends that the definition of CIP Senior Manager found in the NERC Glossary of Terms is updated to reflect the following change:	

*A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through **CIP-014**.* Lastly, Texas RE recommends that CIP-003-8 R1 Part 1.1 is also updated to address CIP-012, CIP-013, and CIP-014. Currently, sub-part 1.1.9 stops at declaring and responding to CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Cleland - GridLiance Holdco, LP - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Guy V. Zito - Northeast Power Coordinating Council - 10	
Answer	
Document Name	

Comment

Incorporating elements of CIP-005 and CIP-010 into CIP-003, when those High/Medium Requirements do not apply to Lows will create difficulty for verifying compliance. For example asset inventory, baseline configuration, patch management activities for Lows. How can the Entity demonstrate compliance for Lows?

The detection of malicious communications requirement is new. It does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services). This is out of this scope.

Without the other layers of cyber security controls, the Entity may not realize they've been compromised.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	
Document Name	

Comment

NRECA continues to believe that NERC and the Regional Entities should undertake at least one year of supply chain standard audits for medium and high impact BES Cyber Systems (which are not even effective until October 1, 2020) before beginning work on supply chain standard requirements for low impact BES Cyber Systems.

This is particularly important when due consideration is given to the recent executive order and potential new regulatory schema/framework for all BES facilities and supporting systems. More specifically, with the recent U.S. President's issuance of a supply chain-focused executive order on "Securing the U.S. Bulk Power System," NRECA is concerned that there could be duplication of efforts relative to Supply Chain risk and risk mitigation. The executive order requires substantial actions relative to future and existing BES facilities and supporting systems and networks. At this time, the extent and scope of this new regulatory schema and framework is unknown and – as a result – conflicts could arise with both the existing supply chain reliability standards and future efforts such as this one. For this reason, while DOE works to develop final rules/regulations by September 28, 2020, this SAR should be delayed allowing time to consider the outcome from the executive order.

NRECA acknowledges the Board of Trustee's resolution to act on these issues; however, the changing regulatory environment since that resolution was passed must also be recognized and presents a significant complicating factor. Given the likely overlap and potential for conflict between the executive

order and NERC's development of supply chain standards, NRECA urges prudency and caution to ensure that efforts are neither duplicative nor conflicting. We look forward to working with NERC staff, industry and DOE to determine the best way forward.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1,3,5 - NPCC

Answer	
Document Name	

Comment

The Taunton Municipal Lighting Plant supports the comments submitted by Brian Evans-Mongeon of Utility Services, Inc.:

Entities are not required to have many of the components of a medium impact CIP compliance program such as: asset inventory, baseline configuration, patch management. The creation of low impact requirements based on the three goals listed in this SAR would be difficult, if not impossible to accomplish without also requiring, if only by inference, that these program components exist.

Concern about the detection of malicious communications requirement since it does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services), which seems inconsistent with determination of low impact.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Since CIP-003 contains elements of CIP-004, CIP-005, CIP-006, CIP-008, and CIP-010, Texas RE recommends the drafting team consider simply listing "Low Impact BES Cyber Systems" in the applicability column of relevant requirements in CIP-004 through CIP-014. Otherwise, the requirements may be effectively duplicated when put in CIP-003.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	
Comment	

IESO supports the comments submitted by NPCC

Incorporating only some elements of CIP-005 into CIP-003, and not the other remaining elements will create difficulty for verifying compliance. Also, without other additional layers of cyber security controls, the Entity may not realize they've been compromised.

The detection of malicious communications requirement is new. It does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services). This is out of this scope.

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	

We appreciate the work that the NERC CIP Standards Drafting Teams are making to develop compliance requirements that improve reliability and security of the Bulk Electric System. We also understand that assets containing low impact BES Cyber Systems are important to protect from malicious activity. That said, the standards development path that low impact BES Cyber Systems are headed for is starting to match the requirements scope for High and Medium impact BES Cyber Systems. Low impact requirements were originally developed and added to CIP-003 to be flexible and less burdensome than the other CIP Standards requirements for High and Medium impact systems.

Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6	
Answer	
Document Name	
Comment	

The Standards Drafting Team shoul give consideration to active remote connections with “vendors” who are contracted to operate a facility, For example, a vendor operating a wind park for a utility from the vendor's control center. The utility is still the GO/GOP.

Likes 0	
Dislikes 0	

Response

Barry Jones - Western Area Power Administration - 9 - MRO,WECC

Answer	
Document Name	

Comment

The term “malicious communication” is a direct borrowing from CIP-005-5 R1.5 for high and medium impact BCS and is based on FERC Order 706 (FERC Order No. 706, Paragraphs 496-503). From a technical perspective, this translates into an entity’s ability to identify ingress/egress protocol traffic to a low BCS, detect and discern known malicious communications protocol packets from non-malicious communications protocol packets and provide a notification, alert or other action in order to “make known” to the entity the malicious protocol packet. This is an activity which is performed by a technology - an Intrusion Detection/Intrusion Prevention System – IDS/IPS and is not based in Policy as requested in the SAR. The inspection (and detection) of ingress/egress protocol traffic for malicious communications could occur at a procedure level, however the process would be manual, time and resource consuming, and have a high frequency of errors. It is therefore infeasible from a policy or process perspective.

Because the language establishes the same requirement at low impact sites as a high or medium impact rated BCS, it will require entities with low impact sites to acquire, install and manage IDS/IPS technologies at low impact sites. This is a significant cost to industry based on a perception of an “aggregate misuse of numerous low impact BCS.”

A recommended option would be to revise CIP-002-5.1 to identify aggregate low impact categorization locations within the criteria of Attachment 1. This would require an entity’s to identify and categorize the aggregate points of low impact sites which potentially are closer to medium than low. If the combined aggregate criteria meets the medium impact categorization rating, the entity will protect the aggregate site or system with security controls commensurate to the aggregate medium impact rating. This utilizes risk as a basis rather than an assumption that *all* low impact sites are an aggregated risk.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 3,4,5,6, Group Name NCPA

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
Thank you for the opportunity to provide comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation (MRRE 80) - NA - Not Applicable - MRO,WECC,Texas RE,NPCC,SERC	
Answer	
Document Name	
Comment	
Emphasis should be given on any new requirements to leverage the significant work that low impact registered entities completed to comply with the CIP-003-7 & 8 focusing on refinement of those processes to reduce vulnerabilities of low impact BES Cyber Systems. Requiring major changes to existing systems greatly increases the timeframe for installation as well as the cost while ignoring incremental refinements that can have a more immediate effect.	

Because these requirements could have a significant impact on pre-existing commercial arrangements, and therefore, consistent with FPA section 215, we ask that the Standard Drafting Team be forward-looking in the sense that the Reliability Standard should not dictate the abrogation or re-negotiation of currently effective contracts with vendors, suppliers or other entities.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
The language for (2) and (3) needs to match what was defined for CIP005-6 R2 Part 2.4 and Part 2.5. This ensures that the standards are consistent for High, Medium, and Low impact BCS that all External Routable Connectivity. Otherwise the language is vague and will lead to ineffective standards.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	

Comment
San Miguel Electric Cooperative agrees with the comments submitted by Barry Lawson of NRECA.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - NAGF - 6 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment
Comments: Emphasis should be given on any new requirements to leverage the significant work that low impact registered entities completed to comply with the CIP-003-7 & 8 focusing on refinement of those processes to reduce vulnerabilities of low impact BES Cyber Systems. Requiring major changes to existing assets greatly increases the timeframe for installation as well as the cost while ignoring incremental refinements that can have a more immediate effect. Because these requirements could have a significant impact on pre-existing commercial arrangements, and therefore, consistent with FPA section 215, we ask that the Standard Drafting Team be forward-looking in the sense that the Reliability Standard should not dictate the abrogation or re-negotiation of currently effective contracts with vendors, suppliers or other entities.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	

Comment
By putting L-BCS subject to many new requirements (for L-BCS at least), the L-BCS inventory becomes an evidence. Responsible Entity must have one. Basically, the BES Cyber Systems should be inventoried. After that, the criteria’s application or not will decide in which category a given BCS is falling: High, Medium or Low. It will be easier to see if the BCS are well categorized and if we didn’t miss something (like a BCS).

By the version 5 of NERC CIP Standards, you did a great effort to reorganize well the requirements from versions 3 and 4. Please, keep the requirements well organized.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
There should be consideration of creating a new CIP Reliability Standard separating required plans and implementations for protecting assets containing low impact BCS from the current CIP-003 Security Management Controls standard. Current reporting options with the CIP-003 R2 CMEP	

activities does not adequately illustrate the extensive protections required, where gaps are identified through CMEP activities, and presents challenges for future growth of low impact protections. There may also be value in updating CIP-002 R1.3 to require a discrete list of low impact BES Cyber Systems. Maintaining an inventory of low impact BES Cyber Systems would mitigate potential risk of inadvertent vendor remote access remaining unprotected. In addition, CIP-003 R1 should be updated to reflect required policy topics for all currently enforceable CIP Reliability Standards (through CIP-014) with updates reflected in the definition of CIP Senior Manager (or just remove the reference to specific standards from the definition).

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

The term "suspected malicious communcations" is slightly vague and could subject an entitiy to additional reporting that does not protect the BES. It may need to be reworded using NIST concepts, terms, and guidance rather than CIP-005 terms.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	
Document Name	

Comment

N/A	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Entities are not required to have many of the components of a medium impact CIP compliance program such as: asset inventory, baseline configuration, patch management. The creation of low impact requirements based on the three goals listed in this SAR would be difficult, if not impossible to accomplish without also requiring, if only by inference, that these program components exist. Concern about the detection of malicious communications requirement since it does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services), which seems inconsistent with determination of low impact.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	
Document Name	
Comment	
Please clarify in the SAR that these new requirements would only apply to sites that allow remote access.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	

Comment
Reclamation recommends adding supply chain risk management requirements to CIP-003-8 or adding low impact BES Cyber Systems to the scope of the documented supply chain cyber security risk management plans required by CIP-013-2. If the required BCS protections are to be extended to include remote access, the standard(s) should require protections against supply chain risks associated with low impact BCS because remote access is more frequently used with low impact BCS. Reclamation also recommends that malicious code detection/protection capabilities do not specifically have to be performed by a perimeter device, but can be performed directly on the asset being connected to (i.e., the Windows host, etc.). If this protection can only be provided by the perimeter device, entities could be looking at significant infrastructure changes. If simply running malicious code protections on their host assets themselves, this would address the security concern. The requirement should indicate “per cyber asset capability.” Running malicious code protections on every conceivable asset is not technically possible; for example, it can’t be run on most PLCs, switches, etc. Reclamation recommends the SAR drafting team thoughtfully assess the cost impacts associated with this SAR to effect changes in a cost-effective manner. The SAR proposes a significant increase in the scope of the affected standards, which will have a substantial impact on affected entities and should not be taken without appropriate consideration. Prior to proposing additional modifications, Reclamation recommends each SDT take additional time to completely identify the scope of each Standard Authorization Request to account for future potential compliance issues. This will provide economic relief for entities by minimizing the costs associated with the planning and adjustments required to achieve compliance with frequently changing standard versions. NERC should foster a compliance environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. To minimize churn among standard versions, Reclamation recommends the SAR drafting team coordinate changes with other existing drafting teams for related standards; specifically, Project 2016-02 and Project 2019-03.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment
RF believes the above can be accomplished by making it additional to CIP-003-8 Attachment 1.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	

Comment
N&ST disagrees with the draft SAR's identification of Project 2019-02 BES Cyber Systems Information Access Management as a related standard or SAR that should be assessed for impact as a result of this proposed project. Neither existing nor proposed BES Cyber Systems Information access management requirements apply to assets containing Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment
"These comments represent the MRO NSRF membership as a whole but would not preclude members from submitting individual comments". The term "malicious communication" is a direct borrowing from CIP-005-5 R1.5 for high and medium impact BCS and is based on FERC Order 706 (FERC Order No. 706, Paragraphs 496-503). From a technical perspective, this translates into an entity's ability to identify ingress/egress protocol traffic to a low BCS, detect and discern known malicious communications protocol packets from non-malicious communications protocol packets and provide a notification, alert or other action in order to "make known" to the entity the malicious protocol packet. This is an activity which is performed by a technology - an Intrusion Detection/Intrusion Prevention System – IDS/IPS and is not based in Policy as requested in the SAR. The inspection (and detection) of ingress/egress protocol traffic for malicious communications could occur at a procedure level, however the process would be manual, time and resource consuming, and have a high frequency of errors. It is therefore infeasible from a policy or process perspective. Because the language establishes the same requirement at low impact sites as a high or medium impact rated BCS, it will require entities with low impact sites to acquire, install and manage IDS/IPS technologies at low impact sites. This is a significant cost to industry based on a perception of an "aggregate misuse of numerous low impact BCS." An option would be to revise CIP-002-5.1 to include an aggregate low impact categorization criterion in Attachment 1 and identify the aggregate points of low impact sites. If the combined aggregate criteria meets the medium impact categorization rating, the entity may be required to protect the aggregate site or system with security controls commensurate to the medium impact rating.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	
Document Name	

Comment
IPL has no further comments.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment
Southern does not have any additional comments at this time.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	
Document Name	

Comment
Rather than a new standard aimed at low impact assets, NERC should put out non-binding guidance to allow smaller utilities to implement protections within their budgetary and resourse limitations.

Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2020-03 Supply Chain Low Impact Revisions

Summary Response to Standard Authorization Request Comments

Introduction

The Standard Authorization Request (SAR) drafting team thanks all who provided comments during the informal comment period. All comments received were reviewed and the identified common themes are addressed below. Some comments have been reserved for consideration during the standard drafting phase of the project. The SAR drafting team will also consider the language of the most recent supply chain standards in the drafting of this standard. As the standard drafting phase begins, the financial impact question and risk will be considered.

The words "vendor" and "third party" are used interchangeably in the SAR and should be consistent.
Based on comments and robust discussion amongst the drafting team, the SAR has been revised (consistent with other CIP standards) to use the term vendor rather than third party.

Terms such as malicious and vendor remote access should be defined.
The need for any new definitions will be discussed and considered during the standard drafting phase.

The SAR could lead to more stringent requirements for Low Impact sites than for other sites and could lead to the possibility of a low impact inventory list being required.
These concerns will be taken into consideration during the standard drafting phase. Reliability standard CIP-005-7 will be closely reviewed, as it is possible that CIP-005-7 R3 (which specifically references vendor remote access) will address part of the concern expressed.

Suggestion to add low impact to the applicability section of all CIP standards.
Modifying the current structure of CIP-003 is outside the scope of the SAR for this team. Comments of this nature will be turned over to the NERC standard efficiency review team to address.

CIP-003-8 Part 1.1 should be updated to address CIP-012, CIP-013, and CIP-014.
Modifying the current structure of CIP-003 is outside the scope of the SAR for this team. Comments of this nature will be turned over to the NERC standard efficiency review team to address.

The proposed standard may result in unfair competitive advantages.
The drafting team does not think the scope in the SAR will lead to development of a standard that poses an unfair competitive advantage for some entities. Furthermore, the scope in the SAR does not preclude any market solutions to achieving compliance with that standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting nominations. Use the electronic form to submit nominations for additional **Project 2020-03 Supply Chain Low Impact Revisions** drafting team members by **8 p.m. Eastern, Thursday, August 13, 2020.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information about this project is available on the project page. If you have questions, contact Senior Standards Developer, Laura Anderson (via email), or at 404-446-9671.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Supply Chain Low Impact Revisions

In adopting the Supply Chain Standards in August 2017, the NERC Board concurrently adopted additional resolutions related to implementation and risk evaluation. These resolutions included preparation of a study of cyber security supply chain risks. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018. In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks.[1] NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or

[1] *See* NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 17, 2019). This report, and the other materials referenced in this item, are available on NERC's Supply Chain Risk Mitigation Program page at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Standards affected: CIP-003-8

The time commitment for these projects is expected to be up to two face-to-face meetings per quarter (on average two and a half full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome. NERC is seeking individuals from ***low-impact entites*** who have significiant subject matter expertise with the Critical Infrastructure Protection ("CIP) family of Reliability Standards and Cyber Asset and BES Cyber Asset definitions. Expertise with of remote access or network design is needed.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	
Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):	
If you are currently a member of any NERC drafting team, please list each team here: ☐ Not currently on any active SAR or standard drafting team. ☐ Currently a member of the following SAR or standard drafting team(s):	
If you previously worked on any NERC drafting team please identify the team(s): ☐ No prior NERC SAR or standard drafting team. ☐ Prior experience on the following team(s):	

Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.
☐ Yes, the nominee has read and understands these documents.

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:		
☐ MRO ☐ NPCC ☐ RF	☐ SERC ☐ Texas RE ☐ WECC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[2] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:			
Organization:			
Name:			
Organization:			

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:			
Title:			

[2] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions

Nomination Period Open through August 13, 2020

Now Available

Nominations are being sought for additional **Project 2020-03 Supply Chain Low Impact Revisions** drafting team members through **8 p.m. Eastern, Thursday, August 13, 2020**.

Use the electronic form to submit a nomination. Contact Wendy Muller regarding issues using the electronic form. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls. Previous drafting team experience is beneficial but not required.

See the project page (linked above) and nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the drafting team in September 2020. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions Observer List” in the Description Box. For more information or assistance, contact Standards Developer, Laura Anderson (via email) or at (404) 446-9671.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security		
Date Submitted:	March 4, 2020		
SAR Requester			
Name:	Soo Jin Kim, Senior Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The project will increase reliability through consistent supply chain protections to low impact BES Cyber Systems. The NERC Supply Chain Risk Assessment Report (December 2019) found that 87% of all BES Cyber Asset locations have low impact BES Cyber Systems, and many of these locations have external connectivity. Currently the systems at these locations would not be subject to the current Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. The impact to the reliability of the BES could be significant if multiple owners and operators allow vendor access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect

Requested information
known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Project Scope (Define the parameters of the proposed project):
This project will address recommendations from the NERC Board resolution from February 2020. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to NERC Glossary of Terms definitions or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Revise CIP-003-8 to include policies for low impact BES Cyber Systems at locations that allow vendor remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions, standards or requirements.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to ~~improve the~~ reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security		
Date Submitted:	March 4, 2020		
SAR Requester			
Name:	Soo Jin Kim, Senior Manager of Standards Development		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☐ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☐ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The project will increase reliability through consistent supply chain protections to low impact BES Cyber Systems. The NERC Supply Chain Risk Assessment Report (December 2019) found that 87% of all BES Cyber Asset locations have low impact BES Cyber Systems, and many of these locations have external connectivity. Currently the systems at these locations would not be subject to the current Supply Chain Standards, CIP-005-6, CIP-010-3 and CIP-013-1. The impact to the reliability of the BES could be significant if multiple owners and operators allow ~~third-party~~vendor access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

This project will address the NERC Board resolution adopted at its February 2020 to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect

Requested information
known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Project Scope (Define the parameters of the proposed project):
This project will address recommendations ~~form~~ from the NERC Board resolution from February 2020 ~~Supply Chain Risk Assessment Report~~. This team will work to coordinate with other ongoing CIP development projects to ensure alignment with any changes to NERC Glossary of Terms definitions or standards and requirements.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Revise CIP-003-8 to include policies for low impact BES Cyber Systems at locations that allow ~~3rd party~~vendor remote access to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impact is unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*., Dispersed Generation Resources):
Submitter asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*., Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Distribution Provider, Generator Owner, Generator Operator
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
Project 2016-02 Modifications to CIP Standards for changes to definitions, standards or requirements. Project 2019-02 BES Cyber Systems Information Access Management for changes to definitions, standards or requirements.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.
None at this time.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
	None identified

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/18/20
SAR posted for comment	04/08/20

Anticipated Actions	Date
45-day formal comment period with ballot	August 2021
45-day formal comment period with ballot	January 2022
10-day final ballot	March 2022
Board adoption	August 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Vendor remote access; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to	containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media	implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor remote access controls but failed to document its cyber security plan(s) for vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2,	Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for vendor remote access controls, but failed to implement vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. Documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - Security Information Management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural or technical controls.
2. Documentation of configuration of security alerts; security alerts or logging relative to activities during the communication from items such as:
    - Firewall policies;

- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;
- manual review of logs; or
- other operational, procedural or technical controls.

3. Documentation showing methods to disable vendor remote access such as:
    - disabling vendor remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - administrative control documentation listing the methods, steps, systems used to disable active vendor remote access; or
    - other operational, procedural or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/18/20
SAR posted for comment	04/08/20

Anticipated Actions	Date
45-day formal comment period with ballot	August 2021
45-day formal comment period with ballot	January 2022
10-day final ballot	March 2022
Board adoption	August 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X~~8~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.
~~All BES Facilities~~.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X~~8~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

~~See Implementation Plan for CIP-003-X8.~~

~~**6. Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;~~ and~~

1.2.6. Vendor remote access; and

~~**1.2.6.**~~**1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

~~1.1.~~ **Compliance Enforcement Authority:**

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~1.3.~~1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

~~The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.~~

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. **Compliance Monitoring and Enforcement Program ~~Assessment Processes~~:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the ~~pruposes~~purpose of assessing performance or outcomes with the associated ~~RELiablity~~Reliability Standard.

~~- Compliance Audits~~

~~- Self-Certifications~~

~~- Spot Checking~~

~~- Compliance Investigations~~

~~- Self-Reporting~~

- ~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~1.6.~~ ~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the ~~six~~ seven

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	of the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to	containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media	implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor remote access controls but failed to document its cyber security plan(s) for vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2,	Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for vendor remote access controls, but failed to implement vendor remote access controls according to Requirement R2, Attachment 1, Section 6. (R2)		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. Documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - Security Information Management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural or technical controls.
2. Documentation of configuration of security alerts;~~,~~ security alerts or logging relative to activities ~~or configuration of security alerts~~ during the communication from items such as:

- Firewall policies;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;
- manual review of logs; or
- other operational, procedural or technical controls.

3. Documentation showing methods to disable vendor remote access such as:
   - disabling vendor remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;
   - disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - administrative control documentation listing the methods, steps, systems used to disable active vendor remote access; or
   - other operational, procedural or technical controls.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber

~~security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~1.1.1 Personnel and training (CIP-004)~~

- ~~Organization position on acceptable background investigations~~
- ~~Identification of possible disciplinary action for violating this policy~~
- ~~Account management~~

~~1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access~~

- ~~Organization stance on use of wireless networks~~
- ~~Identification of acceptable authentication methods~~
- ~~Identification of trusted and untrusted resources~~
- ~~Monitoring and logging of ingress and egress at Electronic Access Points~~
- ~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~
- ~~Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~
- ~~Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access~~
- ~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~1.1.3 Physical security of BES Cyber Systems (CIP-006)~~

- ~~Strategy for protecting Cyber Assets from unauthorized physical access~~
- ~~Acceptable physical access control methods~~
- ~~Monitoring and logging of physical ingress~~

~~1.1.4 System security management (CIP-007)~~

- ~~Strategies for system hardening~~
- ~~Acceptable methods of authentication and access control~~
- ~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~
- ~~Monitoring and logging of BES Cyber Systems~~

~~1.1.5 Incident reporting and response planning (CIP-008)~~

- ~~Recognition of Cyber Security Incidents~~
- ~~Appropriate notifications upon discovery of an incident~~
- ~~Obligations to report Cyber Security Incidents~~

~~1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

- ~~Availability of spare components~~
- ~~Availability of system backups~~

~~1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

- ~~Initiation of change requests~~
- ~~Approval of changes~~
- ~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

- ~~Information access control methods~~
- ~~Notification of unauthorized information disclosure~~
- ~~Information access on a need-to-know basis~~

~~1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

- ~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~
- ~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

- ~~Method(s) for delivery of security awareness~~
- ~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

- ~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

- ~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

- ~~Recognition of Cyber Security Incidents~~

- ~~Appropriate notifications upon discovery of an incident~~
- ~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

- ~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~
- ~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~
- ~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

- ~~Process(es) to declare a CIP Exceptional Circumstance~~
- ~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~Requirement R2:~~

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

~~combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

~~Requirement R2, Attachment 1, Section 3 – Electronic Access Controls~~

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such~~

~~communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

~~The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.~~

~~Electronic Access Control Exclusion~~

~~In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~

~~Considerations for Determining Routable Protocol Communications~~

~~To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.~~

~~When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located~~

~~at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

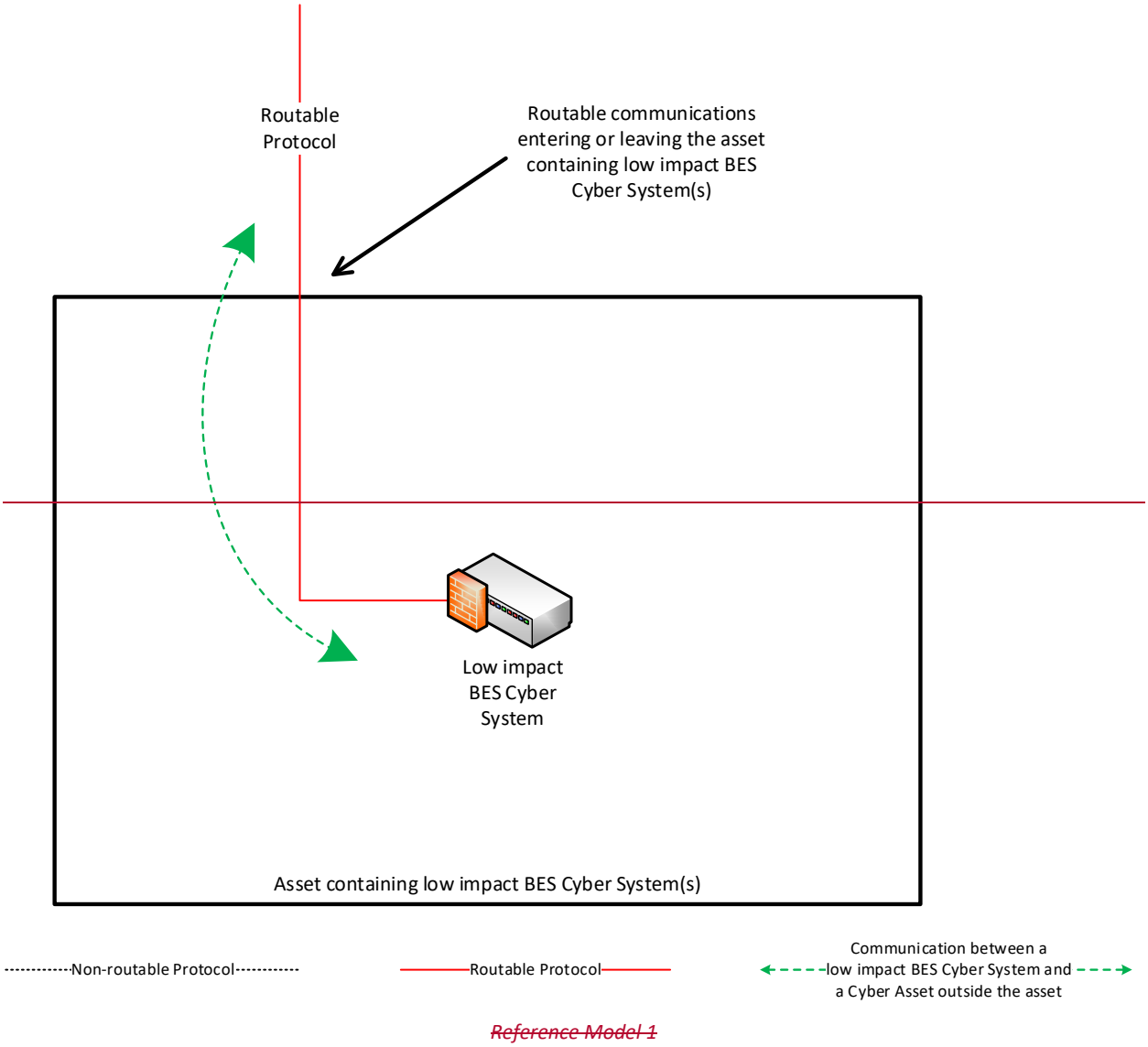
~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

~~NOTE:~~

- ~~This is not an exhaustive list of applicable concepts.~~
- ~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

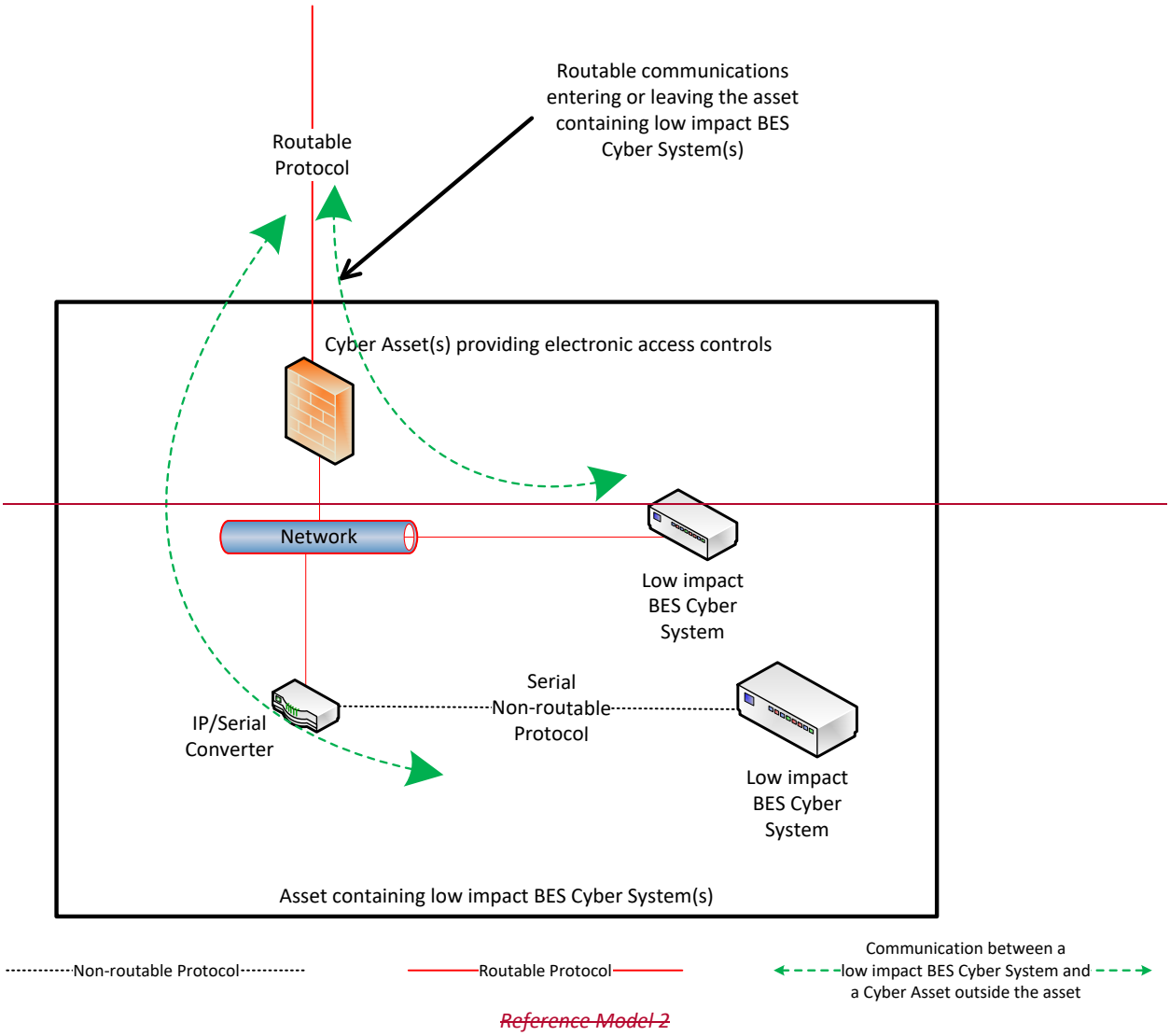
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 1*~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

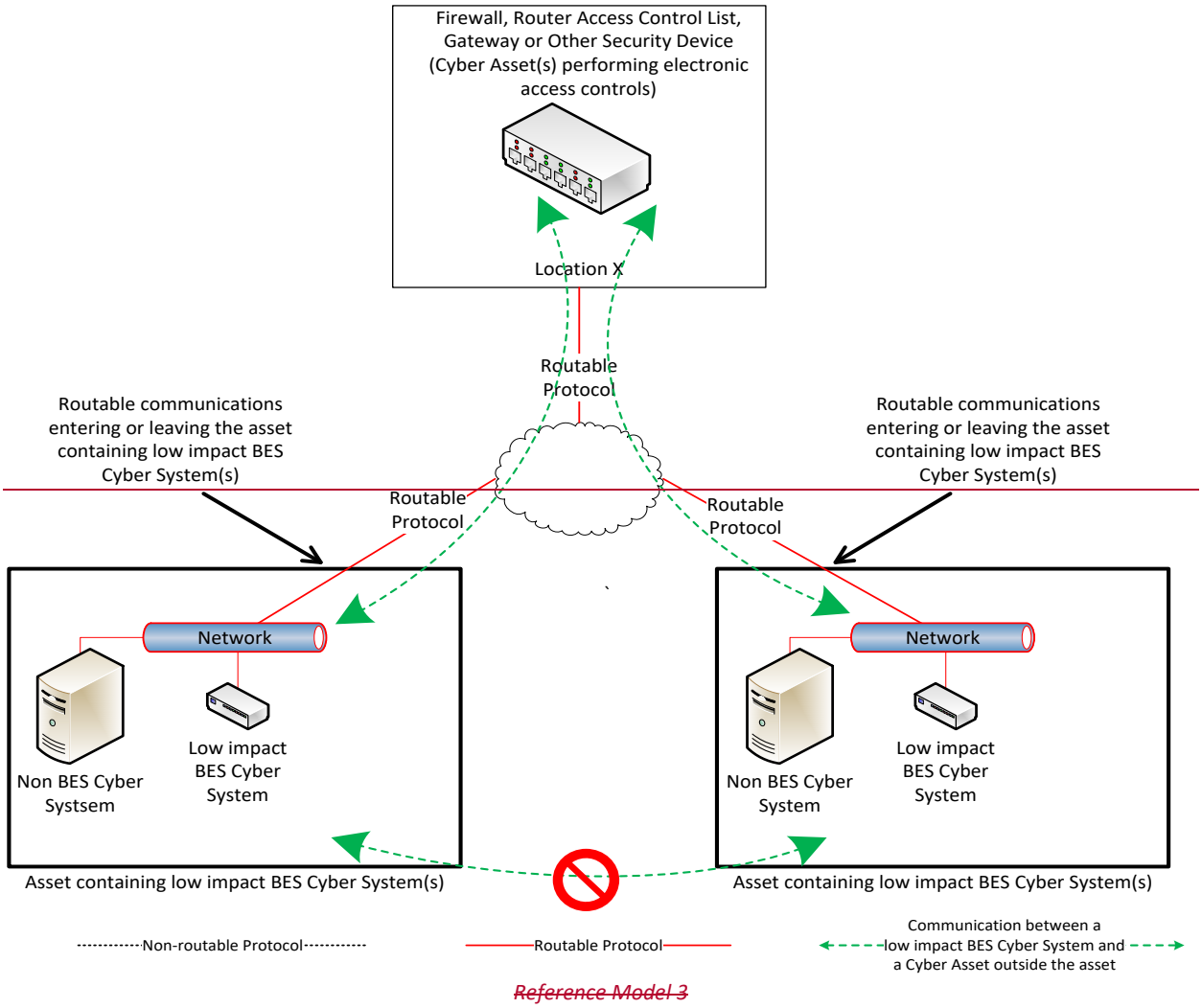
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 2*~~

~~Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

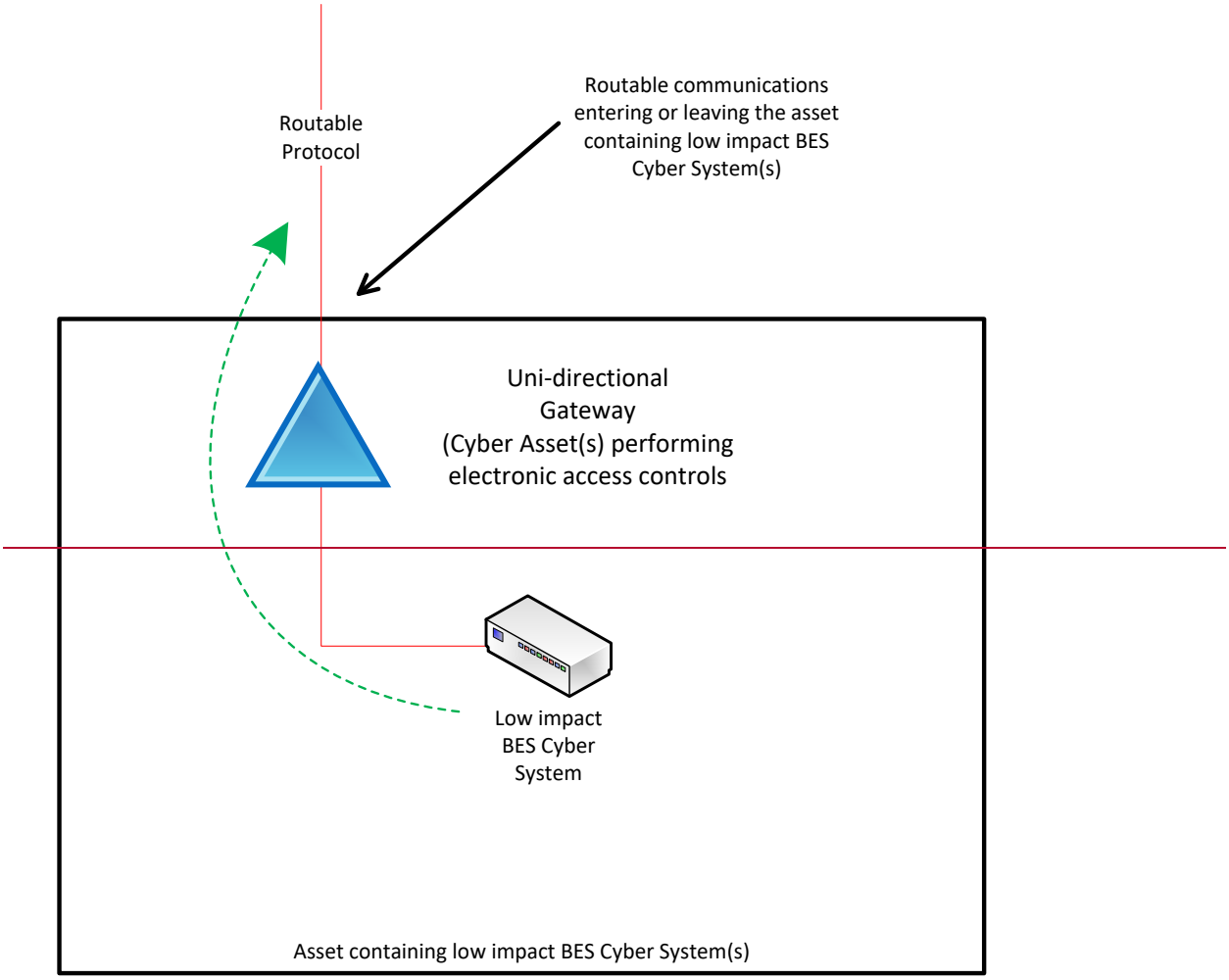
~~The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~*Reference Model 3*~~

~~Reference Model 4 – Uni-directional Gateway~~

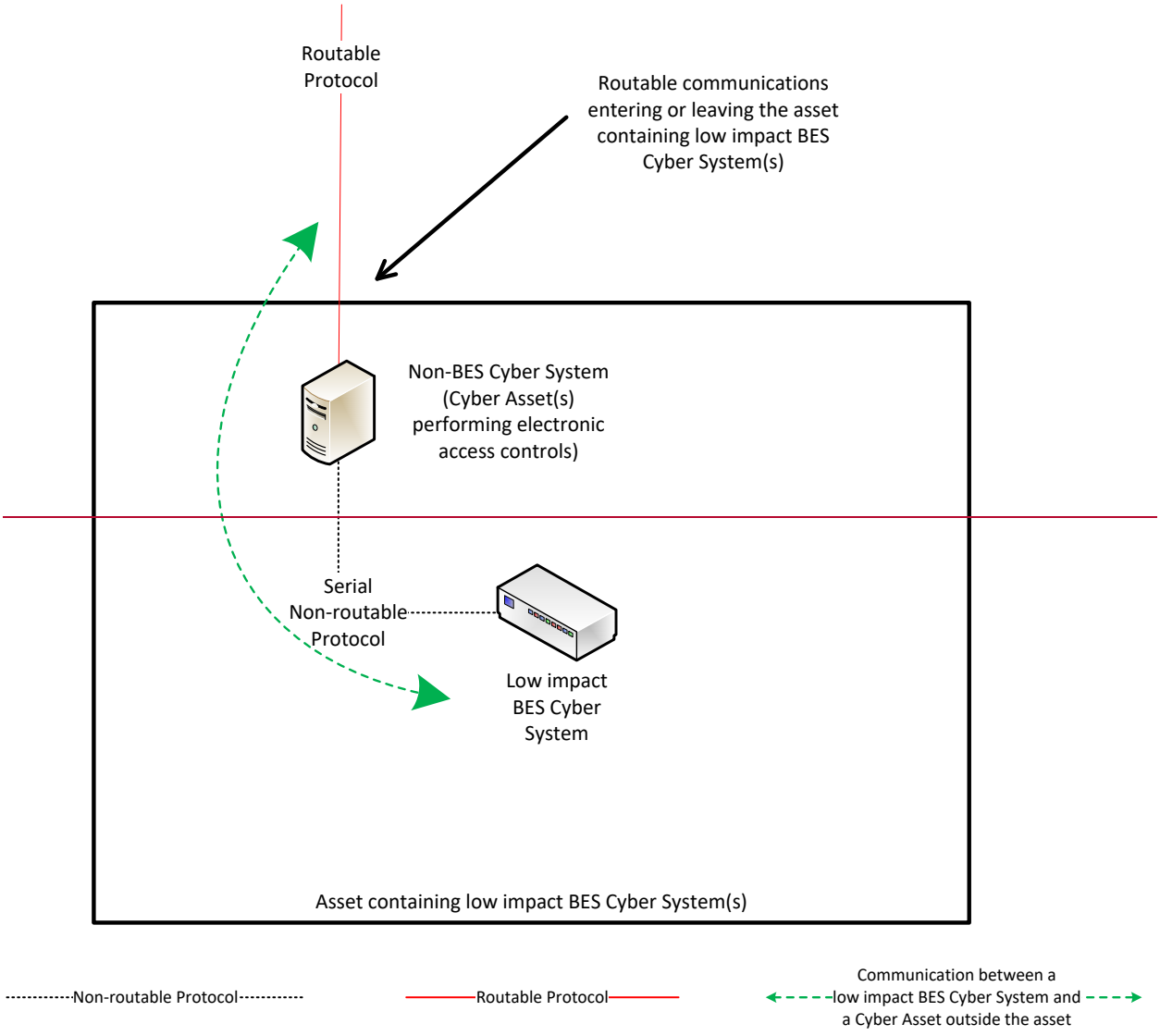
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~



~~*Reference Model 4*~~

~~Reference Model 5 – User Authentication~~

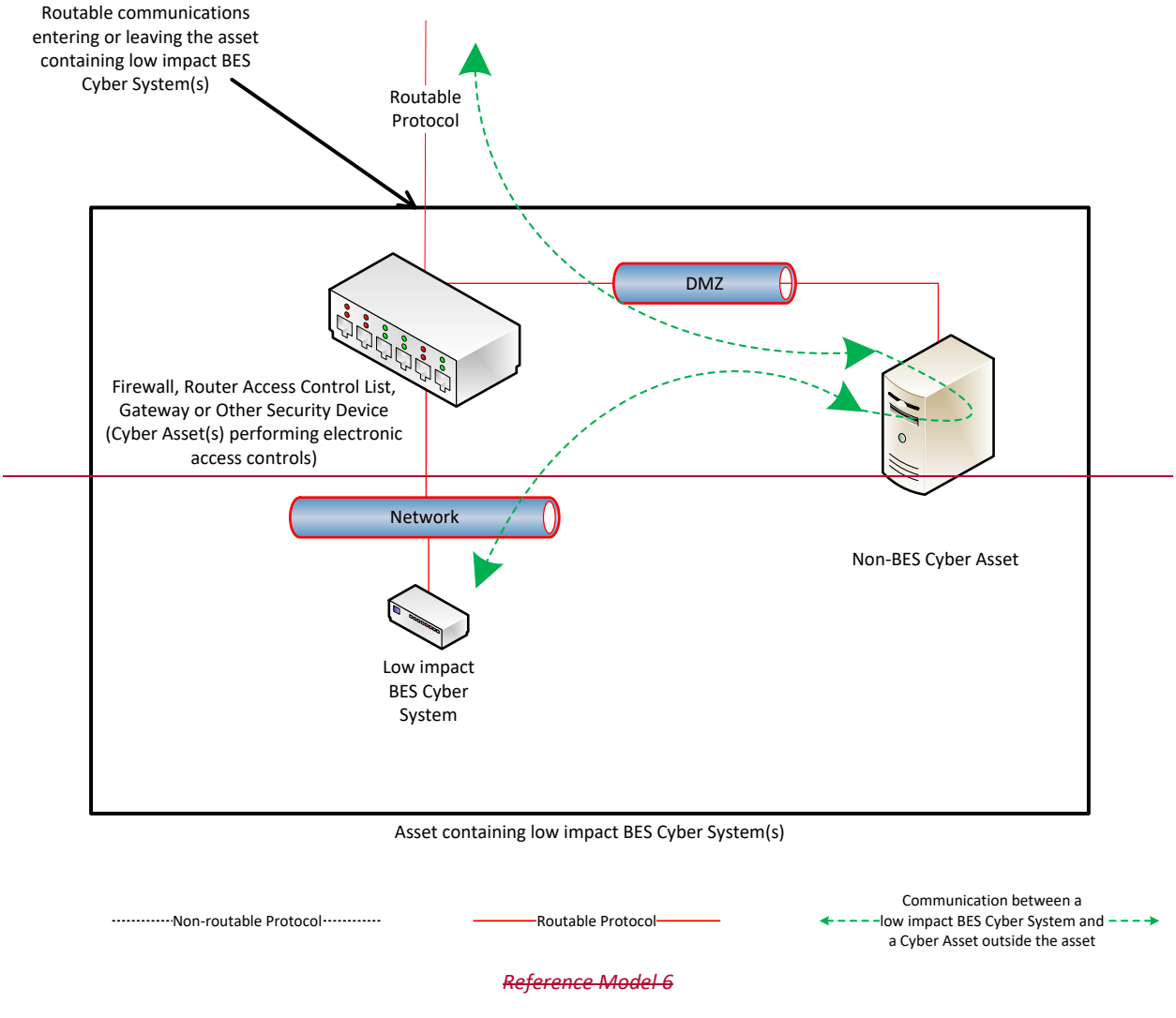
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~



~~Reference Model 5~~

~~Reference Model 6 – Indirect Access~~

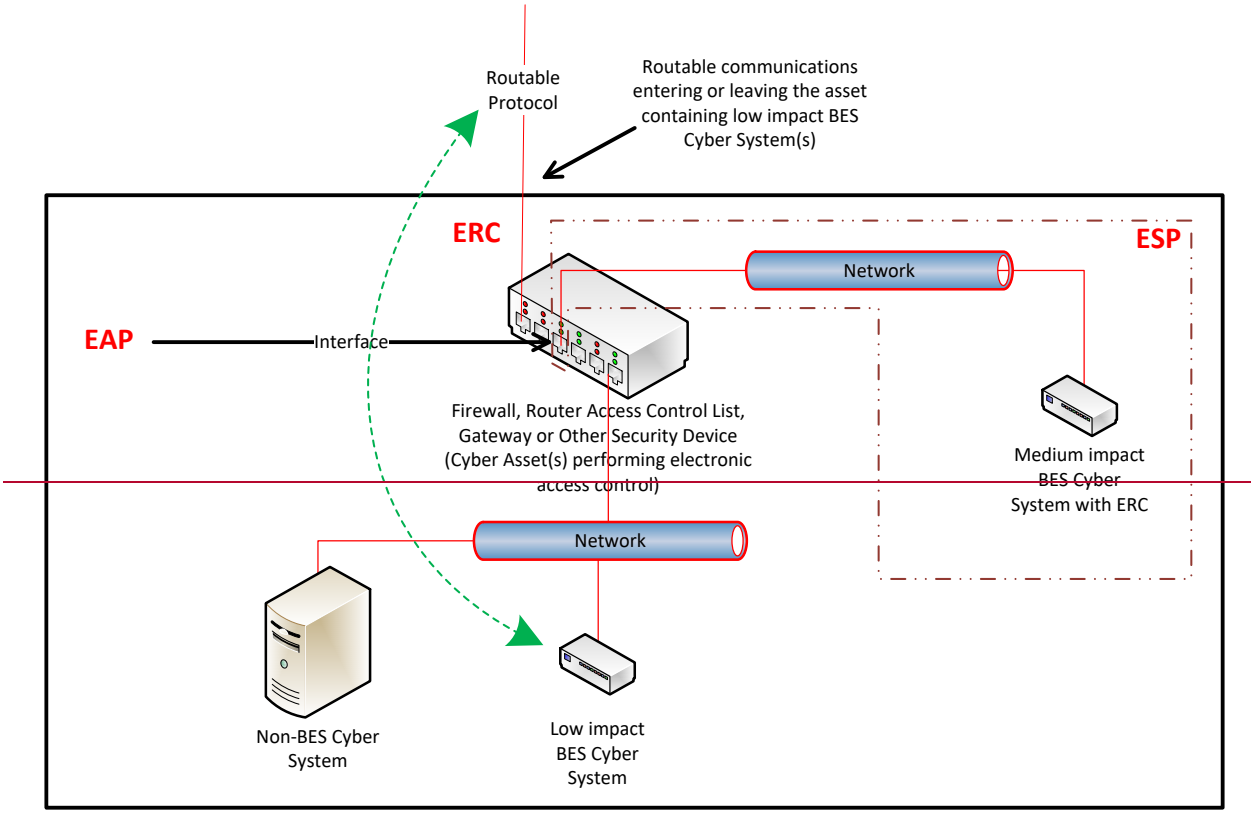
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~



~~*Reference Model 6*~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~*Reference Model 7*~~

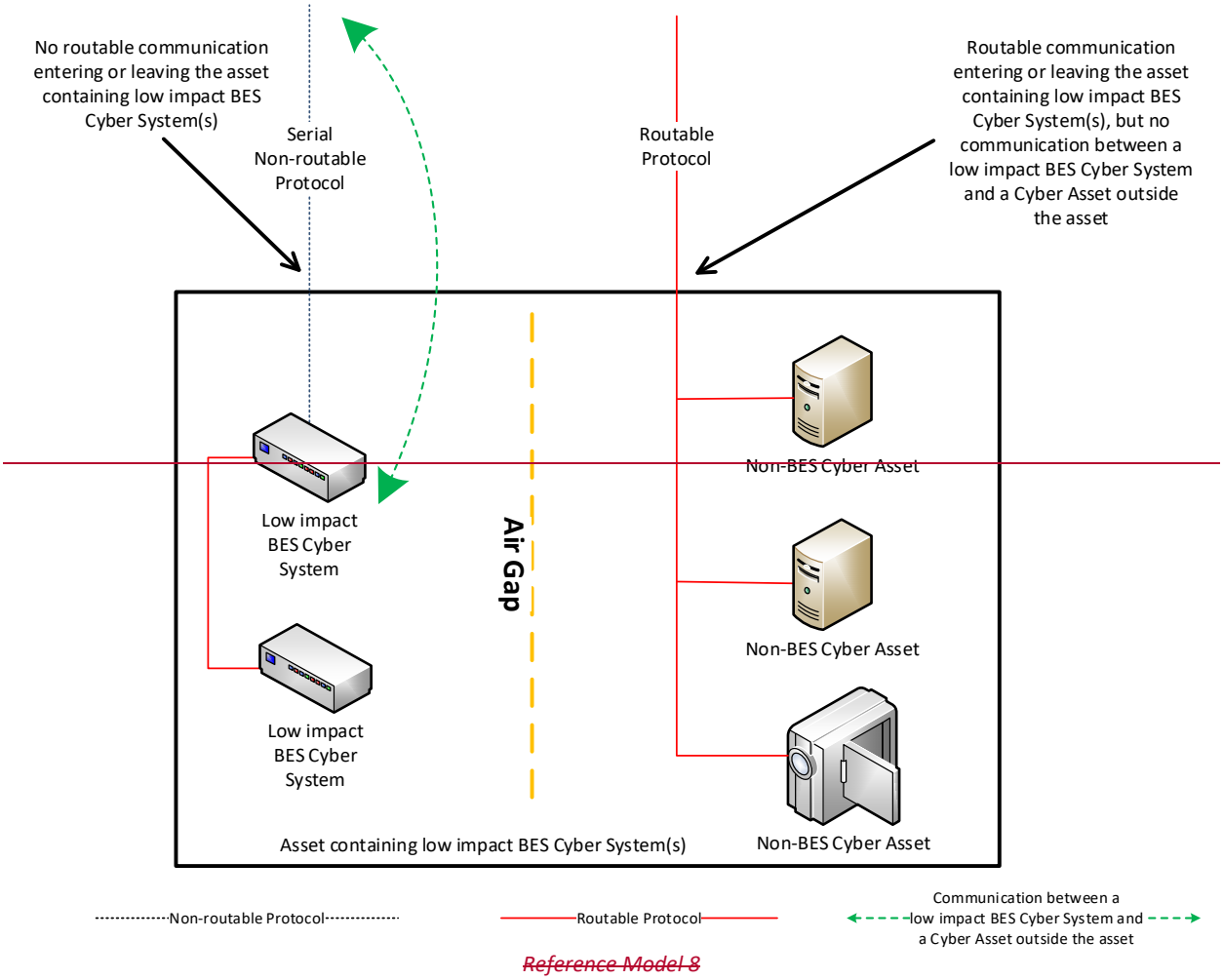
~~Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

1) ~~The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

2) ~~The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

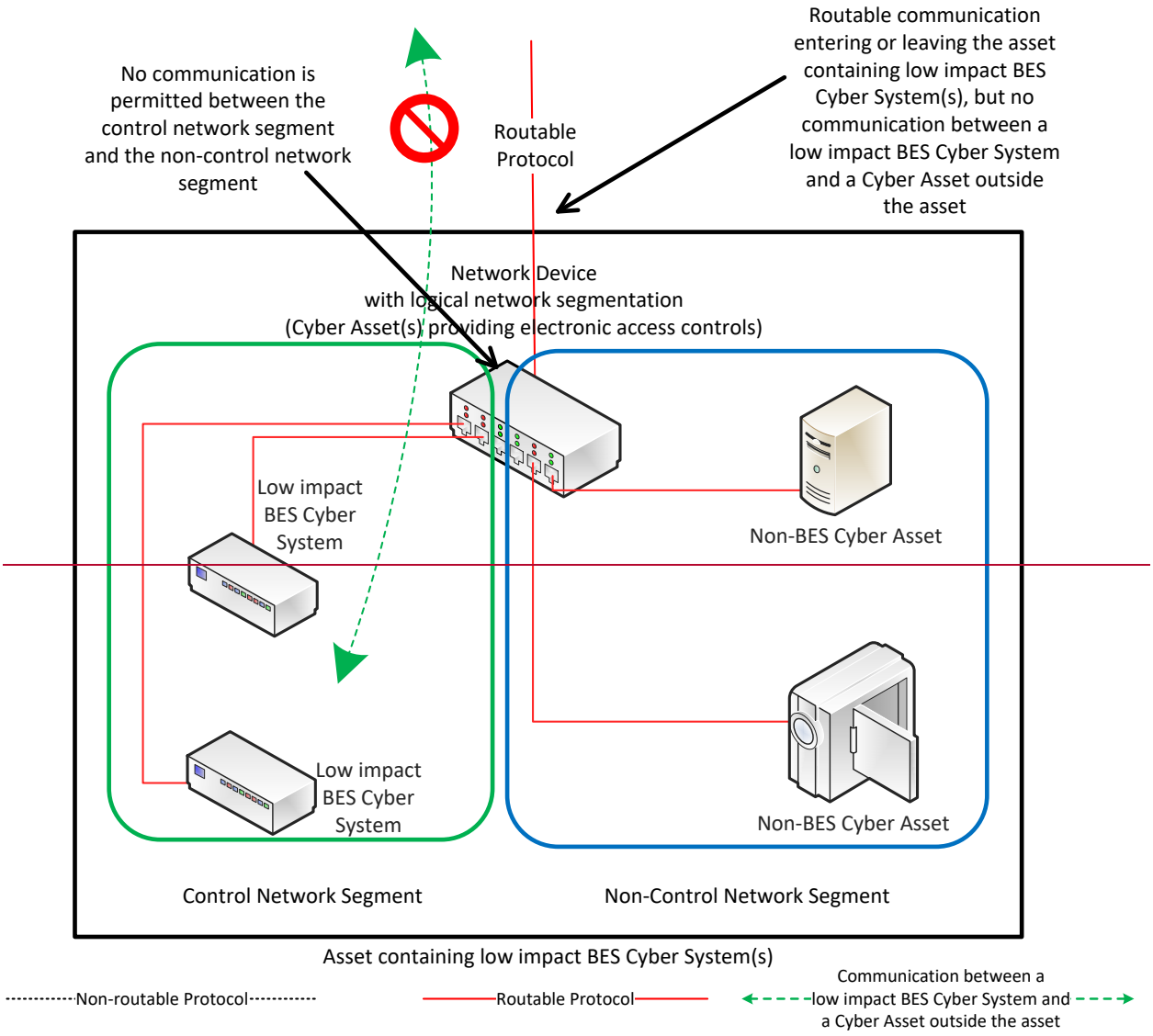
3) ~~The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~



~~*Reference Model 8*~~

~~Reference Model 9 – Logical Isolation – No Electronic Access Controls Required~~

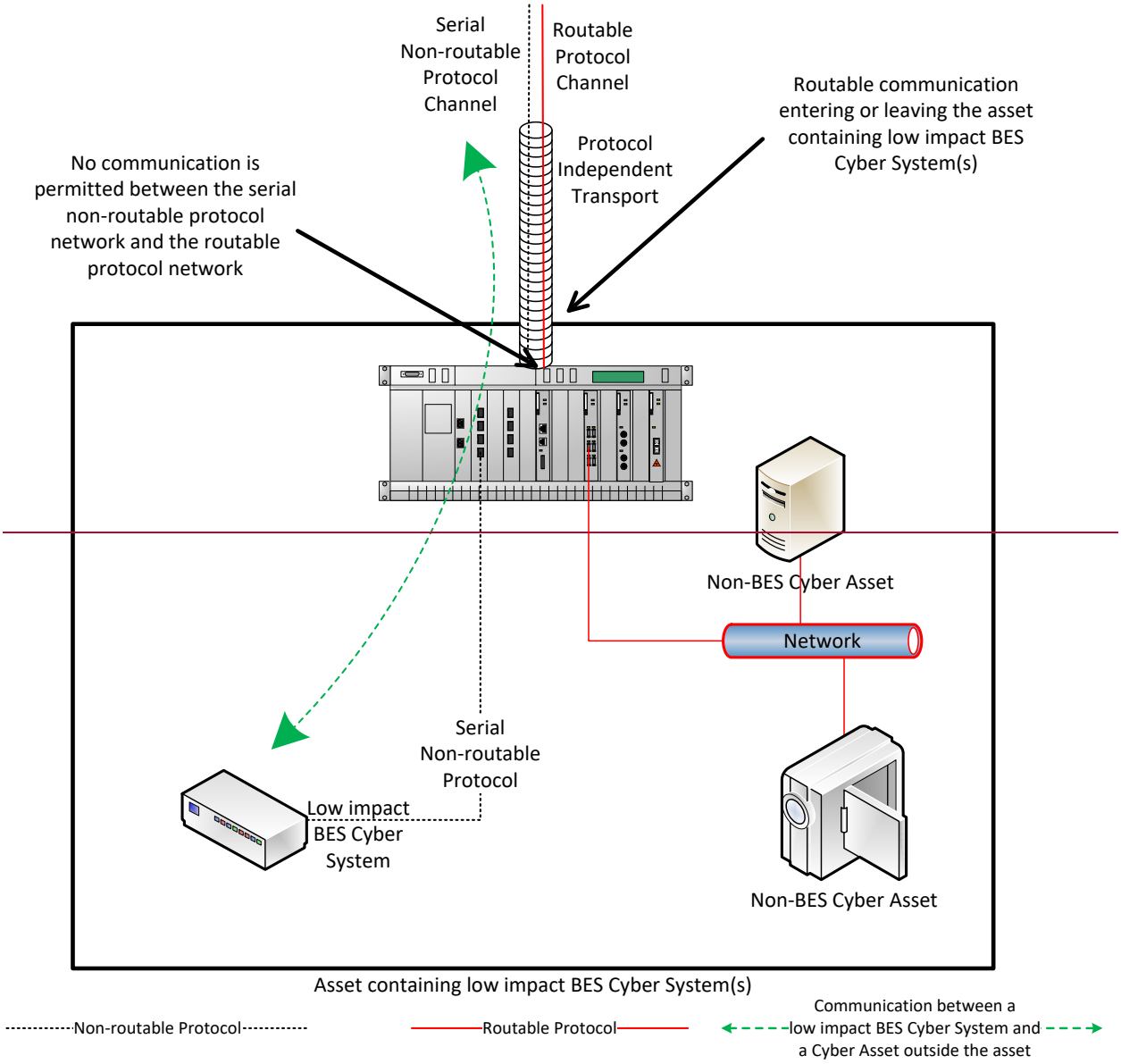
~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~



~~*Reference Model 9*~~

~~**Reference Model 10 – Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required**~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~*Reference Model 10*~~

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

~~disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

- ~~Diagnostic test equipment;~~
- ~~Equipment used for BES Cyber System maintenance; or~~
- ~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

~~Malicious Code Risk Mitigation~~

~~The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~Section 5.1:~~ ~~Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

- ~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~
- ~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~
- ~~When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity~~

Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance

~~Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition

~~and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~Rationale for Section 5 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-X — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date

Reliability Standard CIP-003-X

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2020-03 Supply Chain Low Impact Revisions** by **8 p.m. Eastern, Monday, and October 11, 2021.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Questions

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

   ☐ Yes
   ☐ No

   Comments:

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

   ☐ Yes
   ☐ No

   Comments:

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

   ☐ Yes
   ☐ No

   Comments:

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2020-03 Supply Chain Low Impact Revisions

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-003-X. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-003-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets	than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets	than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the ~~six~~ seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing

identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-012-2 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was modified by adding a seventh topic to Requirement R1.2 for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to review one or more documented cyber security policies covering the topics specified in Requirement R1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-X, Requirement R2
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R2
The VSL did not change from the previously FERC approved CIP-012-1 Reliability Standard.

VRF Justification for CIP-003-X, Requirement R3
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R3
The VSL did not change from the previously FERC approved CIP-012-1 Reliability Standard.

VRF Justification for CIP-003-X, Requirement R4
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R4

The VSL did not change from the previously FERC approved CIP-012-1 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-X

August 2021

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

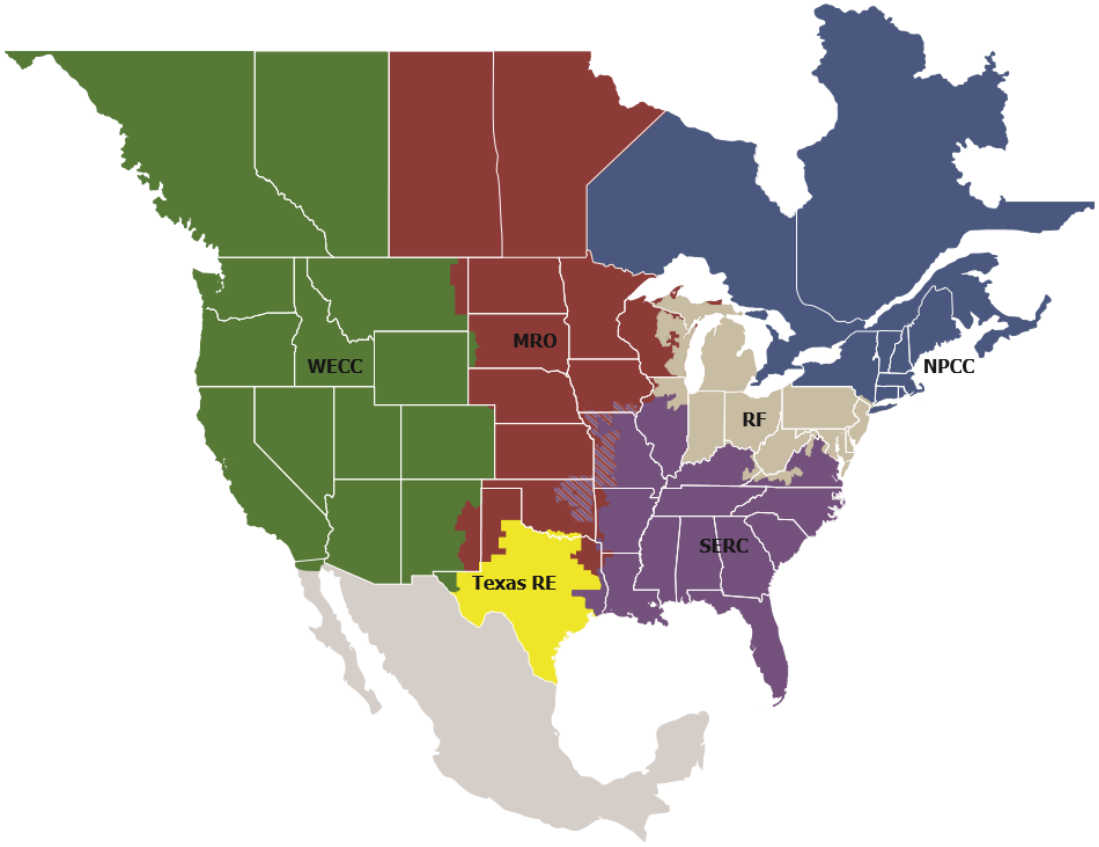
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 67% have external connectivity which often results in the allowance of 3rd party access. As our grid has grown more complex, the use of third parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected; However, the prevalence of external connectivity and 3rd party access, herein referred to as vendor[1] remote access, across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this

[1] Similar to CIP-013, the term *vendor(s),* as used in the standard, is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

vulnerability, the originating FERC Order[2], and the resulting NERC Board resolution[3] the proposed Attachment 1 Section 6, as it relates to the existing Requirement 2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor remote access. This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems.

Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access

The objective of Attachment 1 Section 6.1 is for entities to have visibility of vendor remote access sessions (including interactive remote access and system-to-system) that are taking place on their low impact BES Cyber Systems. Such visibility increases an entities ability to rapidly detect, respond and resolve issues that may originate with or be tied to a particular vendor's remote access session. The obligation in Section 6.1 requires that entities have a method to determine active vendor remote access sessions, R2 requires that said method be documented and implemented.

In support of Attachment 1 Section 6.3, and in line with FERC Order No. 829 (p.49), increased vendor remote access visibility may give Responsible Entities the ability to rapidly disable remote access sessions in the event of a system breach.

Attachment 1 Section 6 Part 6.2 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.2 is for entities to have the ability to detect known or suspected malicious communications such that the entity may respond to and remediate resulting impacts. The obligation in Section 6.2 requires that entities which allow vendor remote access (including interactive remote access) must establish a process/procedure to detect malicious communications from vendors and the systems used by vendors to access low impact BES Cyber Systems. R2 requires that these methods be documented and implemented.

Attachment 1 Section 6 Part 6.3 – Disabling vendor remote access

The objective of Attachment 1 Section 6.3 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52). Per FERC Order 829 (p.49), the inability of a responsible entity to rapidly terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into remote communications and the ability to rapidly terminate a remote communication could mitigate such a vulnerability. The obligation in Section 6.3 requires that entities have a method to disable active vendor remote access sessions, R2 requires that said method(s) be documented and implemented.

[2] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[3] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Open through October 11, 2021
Ballot Pools Forming through September 27, 2021

Now Available

A 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls**, is open through **8 p.m. Eastern, Monday, October 11, 2021**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team will post CIP-003 with a –X version letter at the end and Virtualization will post CIP-003 with a –Y. The version number will be assigned upon adoption by the NERC Board of Trustees.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, September 27, 2021.** Registered Ballot Body members can join the ballot pools here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted October 1-11, 2021.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions (Draft 1)
Comment Period Start Date:	8/27/2021
Comment Period End Date:	10/11/2021
Associated Ballots:	2020-03 Supply Chain Low Impact Revisions CIP-003-X IN 1 ST

There were 82 sets of responses, including comments from approximately 193 different people from approximately 128 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric	1	SERC

						Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Chase Snuffer	Rayburn Electric Cooperative	3	Texas RE
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Jodi Jensen	Western Area Power Administration - Upper Great	1,6	MRO

						Plains East (WAPA)		
					John Chang	Manitoba Hydro	1,3,6	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					Bill Shultz	Southern Company Generation	5	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF

Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC

					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC

					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
Santee Cooper	Tommy Curtis	5		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA acknowledges NERC's concern regarding "aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System." [SAR, p. 1]

BPA agrees with the placement and language of CIP-003-X R1.2.6, as well as Attachment 1, Sections 6.1 and 6.3.

BPA votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium, creating confusion and implementation difficulties. BPA believes that neither the SAR nor NERC's Supply Chain Risk Assessment report* intended to require a higher bar for Low systems than already exist in M/H systems for the following reasons:

1) The Supply Chain report indicates a goal to bring Lows in line with existing M/H requirements: On p. 13 of the Supply Chain report, the summary of Q4 states that the numbers of respondents who do not apply the M/H requirements equally to their Low systems was "contrary to the expectation… that entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems." This points to an intent to copy existing M/H requirements, not add an additional requirement.

2) The SAR is inconsistent, mentioning detection of malicious communications separately from vendor access in the Purpose section, but merging them for “locations that allow vendor remote access” in the Description section.

If the SAR intended for the malicious code requirement to apply to vendor remote access, then Section 6.2 should specify “vendor remote access” to align with 6.1 and 6.3.

If the SAR intended for the malicious code requirement to apply to all remote access, then Section 6.2 belongs in CIP-003-X Attachment 1, Section 3.

However, since there is no equivalent requirement for medium impact BCS, nor any projects to expand CIP-005 R1.5 to all medium impact BCS, then Section 6.2 should be removed entirely to avoid this higher requirement for low impact BCS.

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment

DTE agrees with the placement and language of CIP-003-X R1.2.6

DTE votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium and High.

Further, DTE suggests that CIP-005 R2.4 and R2.5 be modified to include the expanded scope of Low sites under applicable systems.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT add the words “active,” “remote,” and “Interactive Remote Access” to Attachment 1 Sections 6 to align the language with CIP-005-6 R2 and use NERC-defined terms where possible. Section 6 should be moved and included within Attachment 1 Section 3 and not made into a new section and add “If technically feasible” to 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

From: ”Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.”

To: “Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for identifying active vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling active vendor remote access.”

The phrase “determining active vendor remote access sessions” is not clear. The Technical Rationale refers more specifically to ‘when sessions are initiated.

Reclamation also recommends adding “Vendor” to the NERC Glossary of Terms.

Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator

services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

While the language addresses the risk of malicious communication, the term “system-to-system access” is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for “system-to-system access” or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No

Document Name	
Comment	

The Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot.

Below are our concerns with vendor remote access and malicious communication mitigation:

The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions.

In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR?

The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration:

Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining vendor remote access sessions;

6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	
Comment	

While the language addresses the risk of malicious communication, the term “system-to-system access” is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for “system-to-system access” or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI believes the proposed technical requirements are reasonable and address the FERC directive; however, the technical requirements are electronic access controls. The SDT should consider including the following language in a new Attachment 1 Section 3 3.3:

3.3 Implement controls that monitor and restrict vendor remote access that:

3.3.1 Has one or more method(s) for determining vendor remote access sessions;
3.3.2 Has one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

3.3.3 Has one or more method(s) for disabling vendor remote access.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

In general, Dominion Energy supports the comments by EEI.

In addition, Section 6, subparts 6.1, 6.2 and 6.3 do not appear to fully align with the intended mitigations associated with the NERC Board of Trustees’ Resolution dated February 6, 2020. The introduction of the requirement that includes "detecting known or suspected malicious communications" for all low impact BES Cyber Syetems is more stringent than the current requirements for monitoring communications on higher risk "medium" impact BES

Cyber Systems. This more stringent requirement, by definition, lower risk assets does not appear to align with the NERC BOT intent to address the remote access risks for low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
No Texas RE agrees objectives #2 and #3 have been addressed in the proposed revisions. Texas RE is concerned, however, the language proposed in Attachment 1, Section 6 does not address objective #1, “detect known or suspected malicious communications for both inbound and outbound communications”. The proposed language in Attachment 1, Section 6 would require entities to “implement a process to mitigate risks associated **with vendor remote access**,” including “[h]aving one or more method(s) for detecting known or suspicious malicious communications for both inbound and outbound communications.” (CIP-003-X, Attachment 1, Section 6.) Texas RE is concerned that Section 6’s focus on vendor remote access does not capture the full range of malicious communications contemplated under the low impact guidance documents. In the event of a supply chain attack, malicious communications can occur whether or not a Responsible Entity has established an authorized channel for vendor communications. Additionally, in the event of a supply chain attack, malicious communications, such as compromised Cyber Assets attempting to communicate with a Command and Control server, can occur at locations where the Responsible Entity has deliberately not established channels for vendor remote access. Based on this perspective, therefore, Texas RE recommends that the SDT clarify that CIP-003 low impact monitoring obligations extend to **all** inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of vendor remote access. Texas RE recommends moving the proposed language in Attachment 1, Section 6.2 to Section 3 (Electronic Access Controls) so it is clear malicious communication monitoring and detection method obligations apply to all communications, not simply vendor remote access communications.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No

Document Name	
Comment	
Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Suggest interchanging the order of 6.2 and 6.3. 6.2 as is not specific to vendor remote access and it would be clearer to understand the security objectives. To ensure even less confussion consider moving 6.2 to Section 3. The SARs scope of '(1) detect known or suspected malicious communications for both inbound and outbound communications' is not specific to only vendor remote access, but all routable protocol.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	

Answer	No
Document Name	

Comment

The language proposed in CIP-003-X Attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- Context and usage of the term 'malicious communication' needs clarity and BC Hydro proposes to add a definition of the term 'malicious communication' in "NERC glossary of terms" to support the understanding
- Similarly BC Hydro proposes defining and adding term 'vendor remote access' to NERC glossary of terms
- Who and what is considered a 'vendor' also need to be defined in the glossary of terms for clarity and understanding
- The language used in Section 6.2 is referring to 'known or suspected malicious communications'. The use of word 'suspected' is quite open with respect to application and usage. Entities may have varied understanding and consideration of what is suspected and what is not. BC Hydro recommends adding clarity and provide examples of use cases and applicability to improve understanding and to better scope the requirements.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.2 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.2 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.2 completely.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed language and suggests the following edits:

- Attachment 1, Section 6, replace the high level Section 6 language with “Section 6: **Vendor remote access**: Each Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:”
- Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.

Likes 0	

Dislikes 0	

Response

JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment

While AEP agrees with the overall sentiment of the proposed language in Attachment 1 Section 6, we believe it could be modified to provide a more clear understanding of how Responsible Entities are expected to comply. AEP recommends that additional language be included to specify that Section 6 subparts are only applicable to Entities that have implemented vendor remote access as part of their business process. Please see recommendations for language below.

Section 6: Vendor remote access: For low impact BES Cyber System(s) identified pursuant to CIP-002, Responsible Enties that have implemented vendor remote access shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) that include:

6.1 Having one or more method(s) for determining when vendor remote access sessions have been initiated;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment

Malicious communications (whatever that means) has no bearing on access and was not part of the NERC Low Impact report so why is it in this draft? If NERC wishes to address malicous code, it should do it in Systems Administration.

We do not support the use of meaningless phrases such as malicious communications to meet security objectives for compliance. There is a tendency to re-use these phrases by SDT's in an effort to seemingly make it easier to use them because they exist in other areas of the standards however that propoagates a continual mantra of applying something that could mean anything to anyone. Why not just use language for what we are trying to acheive? Another meaningless phrases is system-to-system.

Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy supports EEI comments. Additional analysis would be needed to review the data diode configurations at low impact locations.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy does not agree with the language proposed in Attachment 1 Section 6. Vendor remote access is not a defined term. For this to be an effective requirement this term needs to either be defined in the NERC Glossary of Terms, defined within Attachment 1 Section 6 or a term that is defined in the NERC Glossary of Terms should be used in lieu of it, such as Interactive Remote Access (Please note IRA definition would require modification to apply to low impact). If the Standards Drafting Team (SDT) were to define vendor remote access, Acciona Energy would suggestion the following definition: Vendor Remote Access (VRA):	

Access by a vendor(s) of the Responsible Entity from a Cyber Asset outside the asset containing low impact BES Cyber System(s) that permits remote commands, control functions, software changes or firmware changes (e.g. 'write permissions') of BES Cyber Assets of the low impact BES Cyber System(s).

Using the aforementioned definition for VRA, Acciona Energy would suggest the following Section 6 language:

Section 6: Vendor Remote Access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with Vendor Remote Access to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining Vendor Remote Access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound Vendor Remote Access communications; and

6.3 Having one or more method(s) for disabling Vendor Remote Access.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 1.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

MPC supports MRO NERC Standards Review Forum comments.

Likes 0	
Dislikes 0	

Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
It is difficult to determine if the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems without first defining what “vendor remote access” is. The use of the undefined term “vendor remote access” in CIP-003-9 will cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. The term "malicious communications" should be defined. Is this known malware or does it include any communications to or from an unknown ip address? Would we get penalized for not recognizing a zero day attack? The term "session" should be defined (and maybe "remote session" as well). Is this an active session or any session that is currently defined but inactive (as in through established firewall rules). Could we be penalized for not disabling inactive sessions in the event of an attack?	
Likes 0	
Dislikes 0	

Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF recommends the following additions (**Bold**) to Attachment 1 Section 6, aligning the proposed language with the NERC Board resolution and CIP-005 R2.4 of the NERC Reliability Standards: *Section 6: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with **active** vendor remote access (including **Interactive Remote Access** and system-to-system **remote** access) to low impact BES Cyber Systems that includes:* *6.1 Having one or more method(s) for determining **active** vendor remote access sessions;* *6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and* *6.3 Having one or more method(s) for disabling **active** vendor remote access.*	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, APPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA agrees with several other utility comments that the proposed language is more stringent and not consistent with NERC CIP High and Medium Assets.	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, FMPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, OUC does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	

Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern supports the comments submitted by EEI. In addition, we note Section 6 requires implementation of a process for all assets containing low impact BCS even if no such vendor remote access capability exists. In these instances, it requires methods to determine, detect, and disable a non-existent capability. We suggest the process and implementation of it be made conditional upon such access existing.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
MISO supports the comments of the Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) and thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot. Below are our concerns with vendor remote access and malicious communication mitigation: The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions. In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR?

The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration:

Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining vendor remote access sessions;

6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form (FINAL).docx

Comment

The applicable resolution calls for additional levels of protection; however, the proposed language places an unduly high burden for low impact locations from a cost-effectiveness perspective. In particular, the proposed language effectively requires that the level of protection for low impact assets be effectively equivalent to the level of protection required to be applied to medium-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

OKGE supports EEI comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E agrees with the comments provided by the Edison Electric Institute (EEI) related to the use of the wording “vendor remote access”. Either make this a term in the NERC Glossary or modify Section 6 as indicted in the EEI comments to help in consistency across the industry.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

To clarify and remove ambiguity associated with the BOT recommendations, the term “vendor remote access” should be defined in the NERC Glossary rather than in an attachment to a Standard. Defining “vendor remote access” will ensure registered entities have a consistent understanding of the term in this and other Standards that may use the term.

As an alternative to defining “vendor remote access” in Section 6, EEI offers the following for consideration.

Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: *For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:*

*6.1 Having one or more method(s) for determining **when** vendor remote access sessions **have been initiated**;*

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications:

*6.3 Having one or more method(s) for disabling **active** vendor remote access **when necessary.***

In addition to the above comments, the proposed language in Section 6, part 6.2 is understood to add new requirements that appear to obligate entities to install IDS-like solutions for low impact BCS which is a higher bar than what is currently required for EAPs at Medium impact BCS with ERC. While it is unclear whether this was the NERC BOT's intent, such a requirement raises questions about CIP-005-6, Requirement R1, subpart 1.5.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response, specifically the idea of limiting the requirement to Interactive Remote Access	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State would like to see a definition of vendor remote access either in the Glossary of Terms, Technical Rationale or in the other guides such as the Implementation or the CMEP guides. There is too much misinterpretation surrounding vendor remote access. Tri-State also recommends adding additional language to the term system-to-system to eliminate ambiguity. Proposed language would read ("including interactive and system-to-system **with command-and-control capability access**) ...	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	

Answer	Yes
Document Name	
Comment	

SMUD agrees that the proposed language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems, but believes that it would create less confusion for industry if the a “low impact asset” was referred to as a “low impact facility.” Using lower case asset versus upper case Asset has been a source of confusion since the low impact standards became effective.

SMUD does not believe that CIP-003 R2 Section 6 Part 6.2 belongs in section 6. This requirement may be better suited for Section 3, but should be changed to clearly reflect that the applicability is to vendor remote access (which is not in the current wording as part of Part 6.2). At a minimum, SMUD recommends changing the wording in Part 6.2: e.g.

“6.2 For vendor remote access, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and….”

Regional Entities could potentially interpret 6.2 to increase the scope to have one or more methods for detecting any malicious communications. This could increase the cost to implement and burden of proof to demonstrate compliance. SMUD would suggest adding “vendor remote access” to the requirement so that the scope is absolutely clear.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	
Comment	

: It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	

Comment

PNMR does not agree with industry partners and their recommendation to define "vendor remote access" within the requirements. This definition should be left to the utility.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	Yes
Document Name	

Comment

BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence:

{C}1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;”

{C}2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.”

{C}3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets.

Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	Yes
Document Name	

Comment

Yes, however, the use of the undefined term ‘vendor remote access’ continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term “vendor”. Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	
Comment	

While N&ST agrees the proposed Section 6 requirements align well with the Board's 3-part resolution, N&ST believes they lack sufficient precision and clarity (e.g., would they apply to ANY vendor remote access to assets containing low impact BES Cyber Systems or only to those subject to "Electronic Access Controls" defined in CIP-003-8, Attachment 1, Section 3?).

Likes 0	
Dislikes 0	
Response	

Michael Jang - Seattle City Light - 1

Answer	Yes
Document Name	
Comment	

The use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term "vendor". Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for

Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer	Yes
Document Name	

Comment

It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

It does address the risk, but as written it increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with the adequacy of implementing and auditing. See the response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

CenterPoint Energy Indiana Electric (SIGE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.

Likes 0	
Dislikes 0	

Response

Hao Li - Seattle City Light - 4

Answer	Yes
Document Name	

Comment

Yes, however, the use of the undefined term ‘vendor remote access’ continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of

vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term “vendor”. Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller

Answer	Yes
Document Name	

Comment

BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence:

1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;”

2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.”

3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets.

4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	Yes

Document Name	
Comment	
CenterPoint Energy Houston Electric (CEHE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence: 1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;” 2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.” 3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets. 4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Yes, however, the requirements for malicious communications at low impact are similar to that which already exists in the current enforceable versions of CIP-005-6 Requirement R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for High impact BES Cyber Systems (BCS) and EAPs for Medium impact BCS at Control Centers. The existing CIP-005-6 requirement do not apply to Medium Impact BCS with External Routable Connectivity (ERC). Was it the 2020-03 SDT's intention for this draft of the proposed low impact requirements for malicious communication to impose IDS-like solutions for low impact that are in fact a higher bar than what would currently be required for EAPs at Medium impact BCS with ERC?

Also, the use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, "***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes: 6.1 Having one or more method(s) for determining vendor remote access sessions; 6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and 6.3 Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.***"

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	Yes
Document Name	

Comment

Although the language addresses the NERC Board resolution, it goes too far placing compliance burden beyond requirements established for high and medium impact. Low impact requirements should match the reliability risk. This problem begins in Requirement R1. For medium and high impact, this

point is covered by the defined term Interactive Remote Access which clearly defines “remote access” and includes both vendor and Responsible Entity. For low impact, “vendor remote access” is not defined and allows too much audit subjective interpretation.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	

Vendor remote access can be confused with vendor access via Transient Cyber Asset connected to the Responsible Entity's local network to "remotely" connect to an asset containing low impact BES Cyber Systems (behind physical security controls). "Vendor remote access" must be defined to remove all subjective audit interpretation. Suggest the following: Vendor remote access: for remote routable protocol access originating outside the Responsible Entity's physical security controls for assets containing low impact BES Cyber System via an Internet Service Provider (ISP) from Cyber Assets used or owned by vendors, contractors or consultants…

Likes 0	
Dislikes 0	
Response	

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	

The lack of definition or clarification of the word "remote" might create confusion, please consider adding a definition, either in the NERC Glossary or a standard-specific definition.

The phrase "interactive access" is also confusing and should be further defined/clarified within this document, or a different phrase should be used.

Additionally, the term "mitigate" in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term "mitigate" in the requirement language; but only within the CIP-013 Purpose statement. This makes it appear that the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment
Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3. Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator? Suggest that language be included to specify that remote means physically external to the site to be consistent with the CIP Low Impact protection framework and requirements for communications. Request consistent use of “Low Impact” or “low impact.” The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	

Comment
ITC agrees with the EEI Comment Form response

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	

Comment
Needs to be further clarified

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree Attachment 1 Section 6 only addresses a vendor's access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3, which could allow an interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not. Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	No
Document Name	

Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	No
Document Name	
Comment	
: No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	

Comment
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.

Likes 0	
Dislikes 0	

Response

Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper

Answer	No
Document Name	

Comment
In 6.1 we are required to have "...one or more method(s) for determining vendor remote access sessions." Determining what about them? that they are active or that they merely exist, whether or not they are active. In 6.2 I don't see the benefit of monitoring outbound communications for malicious communications when those communications are only outbound, as with a data diode. the only reason I can think of to monitor outbound communications is as an indicator of response to a remote command & control server. That would only make sense in a two-way communication. In 6.3 I believe that "...disabling vendor remote access" could be interpreted as disabling ALL vendor remote access if any remote access is seen to have malicious communications. If there are multiple sessions ongoing to multiple vendors (as well as employees) we could be found in violation for not shutting down all vendor sessions upon learning that one session is suspicious. In addition we would have to be able to determine which sessions are vendors in order to avoid shutting down employee sessions. Either that or just shut them all down. There is no mention of notifications or timeframe here. Sessions must be monitored but it follows that unless someone is notified in a timely fashion of malicious communications, nothing can be done in a reasonable period of time. And what is a reasonable period of time? A minute, an hour, a day? If we use logging as a method of monitoring, would a daily check of the logs be sufficient. I think we're at the mercy of the auditor on this but those with CIP-005 experience may have a better feel for how this could be implemented and what an auditor might expect.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The SDT has not defined “Vendor” to date. Without “vendor” being defined it is difficult to tell who would be in scope and required to adhere to Attachment 1 Section 6. This is also problematic in regards to Supply Chain for Medium Impact and High impact BES Cyber Systems. We would suggest defining “vendor”.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree Attachment 1 Section 6 only addresses vendor’s access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3 which could allow interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not.

Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5 which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow the use of CIP-003-8, reference model 3.

Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator?

Request consistent use of “Low Impact” or “low impact.”

The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	

To ensure complete clarity, Acciona Energy suggests using a defined term, please see Acciona Energy's answer to question 1.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

Request clarification on "remote" since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. "Remote" could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3.

Request clarification on "remote location." The question includes "remote location" which is not defined. Is the generation switch yard a different location than the generator?

Request consistent use of "Low Impact" or "low impact."

The term "mitigate" in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term "mitigate" in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

Request clarification on "remote location" with respect to BCS

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The terminology of low impact BES cyber systems versus low impact assets needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
It includes malicious communications which has nothing to do with access.	
Likes 0	
Dislikes 0	
Response	
Michael Jang - Seattle City Light - 1	
Answer	No
Document Name	
Comment	
Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	

Answer	No
Document Name	
Comment	

Tacoma Power does not agree that the proposed language clearly addresses vendor's access to low impact assets containing cyber systems from remote locations. Tacoma Power suggests the following edit to Attachment 1, Section 6, Bullet 6.2, "Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and"

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.

Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	
Comment	

As mentioned in comments related to Question 1 above, 'vendor remote access' needs clarity of understanding and clear definitions of the terms for appropriate applicability.

Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	
Comment	

N&ST believes the proposed Section needs to be clear about whether or not it applies only to BES assets containing low impact BES Cyber Systems that are subject to "Electronic Access Controls" defined in CIP-003-8, Attachment 1, Section 3.

Likes 0	
Dislikes 0	

Response	
Brian Belger - Seattle City Light - 6	
Answer	No
Document Name	
Comment	
No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Consider not using ‘a process’ in CIP-003, which is consistent with other Sections of CIP-003. The first part of Attachement 1 speaks to having plan(s). Also suggest using ‘electronic access controls’ as used in other Sections or just ‘controls.’ Consider the following edits for clarification: “Section 6: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit active vendor remote access to low impact BES Cyber Systems, the Responsible Entity shall implement electronic access controls to mitigate risks associated with active vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:” To be consistent with the language of the SAR and CIP-005-6, consider using ‘active vendor remote access’ and not just ‘vendor remote access’ in Section 6, 6.1 and 6.3. From a technical basis it is not clear what would the difference be between the two uses.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

CIP-003 Section 6.2 requirement seems to establish a higher bar than the similar requirement in CIP-005 R1.5 for MIBCS at Control Centers. Additionally, CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low impact BES Cyber Systems”. Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No

Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference “remote locations”.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO supports the NPCC submitted comments	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference “remote locations”.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No

Document Name	
Comment	
Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Attachment 1, Sections 6.1 and 6.3 clearly specify that they apply to vendor access. BPA does not believe Section 6.2 provides the same clarity.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment
PG&E agrees to the language in Section 6 only addresses vendor access to low impact assets containing BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment
It is clear Section 6 only addresses vendor's access to assets containing low impact BES Cyber Systems from remote locations. However, in conjunction with EEI comments on Q1 further clarity on both 'remote' and 'access' is needed. For example, is data from an entity's BCS that is directed through a data diode to physically enforce an outbound only connection to a vendor system included in 'system-to-system vendor remote access'?

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes

Document Name	
Comment	
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD would like to see more clarity regarding what constitutes a vendor. If an entity has contracted with an orgization to operate an asset, are all communications and connections from outside of the asset considered vendor remote access? There are use cases where the entity may contract the operation of an asset that the entity itself has no access to.

Would a contractor, issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor?

The two examples provided are use cases that SMUD feels should not be left up to the region entities.

Likes 2	Platte River Power Authority, 5, Archie Tyson; DTE Energy, 4, ireland patricia
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO Supports the NPCC Submitted comments

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

In general, Dominion Energy supports the comments from EEI.

In addition, Dominion Energy is concerned that when reviewing Attachment 1, Section 6 the current language appears to broaden the scope of applicability to any asset containing the low impact BES Cyber Systems rather than just to the low impact BES Cyber System itself. The language should be clarified to enure that the scope is limitied to just the cyber system and not the entire asset.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Current low impact BCS do not include or required IDS/IPS. The proposed revisions seem to expand the need for them.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	

Comment
Current low impact BCS do not include or require IDS/IPS. The proposed revisions seem to expand the need for them.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language. CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and”

For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed.

Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language.

CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The language in Sections 6.1-6.3 applies to assets that contain BES Cyber Systems. This potentially draws in remote access to non-CIP devices that are located within that asset. The language should be updated to specifically point to the BES Cyber System within the low impact asset. This is different than the way that CIP-003 is written and may need a different Requirement to address.

Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language.	

CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5's Requirement but R1.5 is applicable to High Impact EAP's and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5's Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1

Answer	No
Document Name	

Comment

Section 6 includes "vendor remote access" which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include "vendor remote access". This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

Recommend adding "vendor remote access sessions" to 6.2. For example, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and"{C}{C}

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Language exceeds medium and high impact by not exempting low impact BES cyber systems not having External Routable Communication. This increases scope.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes

Document Name	
Comment	
CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low impact BES Cyber Systems”. Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
While it does limit the scope to low impact BES cyber systems, it does not limit the scope to only those **assets** containing low impact BES cyber systems that permit vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for: **Attachment 1 Section 6:,** **Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:** **6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;**	

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement "**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**".

Likes 0	
Dislikes 0	

Response

Michael Jang - Seattle City Light - 1

Answer	Yes
Document Name	

Comment

The use of the term 'vendor remote access' continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement "***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***".

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	
Comment	
It does because CIP-003 is applicable only to Low Impact assets (not Cyber Systems)	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
The language implies that additional analysis is required for vendor remote access once an analysis was performed.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Yes, NERC Reliability Standard CIP-003-8, Attachment 1 is only applicable to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

SIGE agrees the language in Attachement 1 Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF has no comments.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

APPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	

However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”.

Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	

FMPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	Yes
Document Name	

Comment

OUC suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern believes the language in CIP-003 R2 makes it clear that all sections in Attachment 1 are limited in scope to low impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E believes the language of Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, “***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact***	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cost can vary widely depending on interpretation of vague language.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
At this point, we believe the framework still requires significant modifications before assessing the cost effectiveness of the proposal.	
Likes 0	
Dislikes 0	

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 0	
Dislikes 0	

Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC does not agree with the EEI response. ITC believes that this requirement is NOT as cost effective and would require specialized equipment and/or processes.	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional consideration needs to be given to the Virtualization project and flexibility that access approach can allow	
Likes 0	

Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment
At this time PG&E does not have information to determine if the modifications are a cost-effective approach. PG&E would have preferred to answer this as un-known and not “No”, but that option does not exist within the NERC Standards Balloting and Commenting System (SBS).

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment
Due to the number of assets potentially affected by the proposed changes as well as the complexity of the proposed measures, implementation of proposed language would be disproportionately costly to implement given the risks associated with low-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

MISO supports the comments submitted by the MRO NSRF and does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller

Answer	No
Document Name	

Comment

BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	
Comment	
NCPA does not agree it's cost effective for Low Impact Assets to be subjective to more stringent requirements than NERC CIP High and Medium impact Assets.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The cost and implementation could be quite significant if entities were to have to renegotiate contracts and put in place remote vendor access controls for remote low-impact facilities The cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Low impact environments are often unmanned and lack the types of infrastructure required for determining, detecting, and disabling malicious activity (IDS, IPS, SEIM, Intermediate Systems, etc…). These new requirements could potentially expand the scope of existing low impact programs with respect to cost for new monitoring functionality.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	
MPC supports MRO NERC Standards Review Forum comments.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy does not believe that the modifications will be cost effective within the current scope of the implementation plan. The cost of deploying security measures to meet the requirements within an 18 month time frame at hundreds of low impact substations and other assets will be a strain on entities budgets and existing IT/OT security personnel. Evergy suggests spreading this effort out across a longer time frame of 36 months or more to be less impactful financially and more realistically achievable.	
Likes 0	
Dislikes 0	
Response	

Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Many entity's will believe that "malicious communications" translates to Intrusion Detection Systems for Low Impact assets. That could translate to $millions for entity's.	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends editing the language in Attachment 1, Section 6, Bullet 6.2 in order to provide a more cost effective approach. Instead of detecting, Tacoma Power proposes changing the measure to monitoring for malicious vendor remote access communication, as follows: Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Although the cost may differ between entities, it's impact may change based on understanding & clarity of terms and scope of application. As advised in comments of Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However requirement in CIP-003-X Section 6.2 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5 where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS. Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes that a considerable amount of research would be needed before many respondents would be able to provide a well-informed answer to this question. We note that the December 2019 “Supply Chain Risk Assessment” report states, “More than 99% of the responders (to a survey question about costs and benefits) agreed with the draft response that it was premature for CIP-013 registered entities to determine or estimate costs or benefits	

associated with the implementation of the standard…" That said, N&ST believes the cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	

Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The broad scope of the proposed language appears to bring all low impact assets into scope as it requires all communication to all assets be monitored at alkl times for malicious communication through vendor remote access, whether the access is being utilized or not.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost effectiveness of the approach to compliance cannot accurately be determined.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The MRO NSRF does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	

Comment
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost-effectiveness of the approach to compliance cannot accurately be determined.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	

Comment
Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No

Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends this project may be a good avenue to incorporate low impact requirements into these standards to avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to. Cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA does not believe that adding an additional requirement to Low systems over current M/H requirements is cost effective.	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Given the ambiguity around what constitutes “vendor remote access” it is difficult to determine what it would take to comply with the proposed requirements or determine if the modifications would be cost effective. Would a contractor that is issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor? The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
TMLP believes that the cost of implementing these additional protections will not be overly burdensome in the sense of adding equipment, but the time that it takes to complete small daily/regular tasks may be increased and therefore may increase labor expenses.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF’s comments for Question 4.	
Likes 0	
Dislikes 0	
Response	

Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP agrees that the proposed modifications are cost-effective so long as a couple criteria are met: • The proposed language AEP has suggested in response to Question #1 is incorporated in Attached 1 Section 6. Proving the negative is burdensome to the Responsible Entity, and the proposed language will ensure Responsible Entites are not required to do so should they not have vendor remote access implemented as part of their business process. Please see AEP's response to Question #1 above. • The solution to meet the vendor remote access requirements can be implemented at the network or perimeter level rather than at the device or substationlevel.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel/vendors appropriately.	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
We do not believe that the technology exists to identify and deter in real time any risky communications by the OEM when interrogating the DCS, nor is it likely to become available in the next eighteen months.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO supports the NPCC submitted comments.	
Likes 0	
Dislikes 0	

Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI recommends a 24-month impelemntation plan given the large vendor solution diversity within a very non-homogenous array of low-impact facilties. Entities may need to compile a inventory of applicable Cyber Assets to determine the impact of the proposed requirements as entities are currently not required to maintain a discrete listing of Cyber Assets at low impact facilities, which are most likely to contain multiple vendor solutions. This extended implementation plan provides entities sufficient time to conduct an inventory of applicable BCAs and BCSs, and implement additional electronic access controls which may be both procedural and technical in nature.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy generally supports EEI comments. A minimum 36 month implementation period, based on the current broad scope of the proposed standard impacting DERs, which are rarely manned but have remote access for operations, would be necessary to design, install, and train for new equipment and capabilities.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the time, effort, and cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3. N&ST recommends a 24 month implementation time frame.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends a longer implementation plan e.g. ~ 36 months considering the cost and scope impact as identified in comments of Question 4 and 1 above. Once the clarity of terms and definitions as identified per our comments to Questions 1 and 4 is obtained, BC Hyrdo will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	No
Document Name	
Comment	
The requirement to review and affect changes need a longer duration to implement. An implementation plan of a minimum of 36 months to complete the changes. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Recommend a 24-month implementation	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We suggest 24 months because of the number of assets with low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations will take much more time.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

Recommend a 24-month implementation due to the significant scale of Low Impact.

As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

MPC supports MRO NERC Standards Review Forum comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

With most entities budgeting 18-24 months in advance, for new infrastructure and staffing resources, this could be a problematic timeline. The Entity would need to update their processes, procedures, train staff, hire resources, and implement technology. All this would need to be completed once budget has been approved. Based on Entity budgeting and the multiple items that will need to be address we would suggest 24-36 months.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No

Document Name	
Comment	
The NAGF recommends that the proposed implementation plan be modified to allow for 24-36 months following the effective date. This timeframe will allow entities to implement the necessary hardware/software, procedural, and vendor contract changes at low impact facilities.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See comment provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA suggests that 24 months be given for implementation to procure, configure, install, train and write procedures associated with the task of detecting malicious communication.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	

Answer	No
Document Name	
Comment	
Presently, there is no requirement obligating a "low" asset list. We believe that these changes would require compiling a detailed list. In our opinion because we have a vast amount of low Cyber Systems, 18 months would not be adequate time to compile and validate such a list.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS feels that a 24-month implementation plan would be a reasonable timeframe to implement process, procedures or technology to meet the proposed language in Section 6. It may be necessary to design and implement multiple solutions to meet the proposed language in Section 6 across the various environments in which low impact assets are in use. Alternatively, a single solution which could be applied across a broader group of low assets may require significant design changes to process, procedures and/or technology.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations may take much more time. CEHE recommends a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports comments submitted by the MRO NSRF. The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	

Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Due to the number of assets potentially affected by the proposed changes and high likelihood that additional technical controls will need to be implemented, 18 months would not be adequate to implement the proposed measures. To allow for budgetary allocation and implementation for technical measures needed to comply with the proposed changes, GSOC recommends a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
OKGE supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
18 months is not adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to implement substantial new protections for low impact BES Cyber Assets in order to monitor and control vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess & document vendor-specific remote access at all of their affected facilities, which is a significant undertaking. Given the current supply chain issues/delays underscores the substantial and impacts on entities' ability to timely secure materials necessary to implement these changes. For these reasons, the implementation plan should be a minimum of 36 months.	

In addition, Attachment 1, Section 6, part 6.2 could be understood to require entities to install IDS-like solutions for low impact BCS. Given the large number of locations and the efforts that will be required to implement 6.2 and the aforementioned supply chain delays, 36 months is more than reasonable . While a phased approach may be another solution, the logistics of effectively implementing a phased approach will be difficult to both budget, administer and audit.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional time of 24 months due to potential funding cycles needed for implementation	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment
Recommend a 24-month implementation due to the significant scale of Low Impact. As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment
If the scope is clear, 18-months for implementation should be fine. Given some of the ambiguity in the current draft, more specifically, the lack of clarity of key terms, it is difficult to determine the extent of changes or what additional technical resources necessary to comply. Additionally, some entities may have very limited security technologies in place for or at low impact assets that can be re-used for the purpose of meeting the requirements. For those entities, it may take much more time to architect, procure, and deploy a solution. Given the potentially large number of low impact sites, 18-months could be challenging.

Likes 0	
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	Yes
Document Name	

Comment
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.

Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP believes the 18-month implementation plan allows for enough time so long as: • the requirement is applicable to Responsible Enties that have implemented vendor remote access as noted in the response to Question #1, and • the solution to meet the vendor remote access requirements can be implemented at the network-level rather than at the device-level as noted in our response to Question #4. Should that not be the case, a 36-month implementation plan would be more appropriate.	
Likes 0	
Dislikes 0	
Response	
Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF’s comments for Question 5.	
Likes 0	
Dislikes 0	

Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes the 18-mont implementation plan can be achieved base on our current setup but understands the concerns raised in the EEI comments related to supply chain delays for other entities and would be willing to support a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Our specific system will not have a problem trying to meet an 18-month implementation plan, but we do have some concerns for the entire Low Impact category due to the large amount of entities who fall under this category, and the varying degree of size and abilities of the entities who fall under this category. Some entities may be less equipped to handle these issues than others.	
Likes 0	

Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	
Document Name	
Comment	
Unable to comment on this.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	

Tri-State does not agree with an 18-month implementation plan. Again, applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations. A longer phased-in approach would be more appropriate for planning and budgeting purposes. Tri-State suggests a 36 month phased-in approach.

Likes 0	
Dislikes 0	

Response

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.	
Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	
Comment	
I also support comments provided by Utility Services.	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	
Document Name	
Comment	
TMLP believes that it may be necessary to require the vendor provide the Registered Entity with logging information about who and what was done during the remote session. While we recognize that this was listed as one of the options in the CIP-003-X Attachment 2 for Section 6, we believe that this should be required in some manner.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.	

a. “Remote” would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find “3rd party” in the CIP-013 documents.

c. Where is the rest of the old “Guidelines and Technical Basis (GTB)?” We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.

a. The technical rational (TR) for 6.2 states: “The obligation in Section 6.2 requires that entities which allow vendor remote access.” We request updating the Requirement by adding “vendor remote access.” To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase “active vendor remote access sessions”. 6.1 and 6.3 do not include the word “active”. Without the word ‘active’, 6.1 and 6.3 could include or maybe be limited to “capability” of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses “that are taking place” and the TR for 6.3 uses “active”. Sections 6.1, 6.3 and the TR should consistently use the word “active”.

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA’s. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	

Comment
The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. ATC requests the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements. Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. ATC requests consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment
As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures. BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	

ITC prefers to retain the Technical Rationale, especially verbiage that limits scope to Low Impact and Interactive Remote Access.

Furthermore, ITC believes this requirement is not as cost effective as mentioned by EEI. In Section 6.2 a requirement to scan traffic for suspicious, malicious communication requires specialized equipment and/or processes. Today, this is only necessary under CIP-005-6 R1.5 for High Impact. The impression is that we're talking about skipping Medium and going to Low. This does not appear to follow a risk based approach.

Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI also notes that the SDT did not request comment on the modifications to Requirement 1, subpart 1.2 which is material to the draft. In the modifications to this section, we note that the SDT has used the undefined term “vendor remote access”, while leveraging this key term in both Requirement 1, subpart 1.2.6 and Attachment 1, Section 6 even though this term is not well understood by the industry. EEI recommends defining of this term. (See our comments to Question 1)

Additionally, EEI believes it may be more efficient and effective over time to simply reference all parts of Attachment 1 within Requirement 1, subpart 1.2 rather than modifying Requirement 1 each time changes are made to the requirements associated with CIP-002, containing low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	

We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions:

While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS.

Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E has no additional comments on the modifications.

Likes 0	
Dislikes 0	

Response

Sarosh Muncherji - British Columbia Utilities Commission - 9

Answer	
Document Name	

Comment

There is the usual direct supply chain where specific vendor products are utilized for BES cyber system operations and maintenance. There are other sources of software that may possibly be overlooked as being part of the "supply chain" and these products may slip through the cracks. Examples include freeware utilities such as text editors (for example, NotePad++) and communications programs (for example, PuTTY). The SDT may consider requiring software integraty validation for all software in a future revision to the standard.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

Of significant note, the proposed changes do not reference protecting only a routable communication medium, leaving the language unclear as it relates to non-routable connections as might be found in low-impact field equipment. Similar requirements in medium-impact systems are only required at Control Centers as reflected in CIP-005 R1.5 or are otherwise qualified based on the connectivity of the cyber asset, e.g., CIP-005-6, R2.4, R2.5. Thus, the proposed requirements for low-impact assets require greater protections across a larger swath of assets than the ones governing medium-impact assets. The proposed language, therefore, raises the protections of low-impact assets to that of high-impact assets, thereby removing any risk-based differentiation of controls between impact ratings.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	
Document Name	

Comment

Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response

LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman

Answer	

Document Name	
Comment	
Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	
Document Name	
Comment	
As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures. BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	

We request that the Guidelines and Technical Basis are not removed from the standard. The Technical Rationale document released with these changes only addresses the new Section 6 changes, and does not replace the comprehensive Guidelines and Technical Basis currently in the standard. The current Guidelines and Technical Basis are used as reference documentation by NERC Regional Entities and Generator Owners, and we believe have played a critical role in the development of compliance programs and internal controls.

Likes 0	
Dislikes 0	

Response

Hao Li - Seattle City Light - 4

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

Comments: Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker
Answer
Document Name
Comment
See comment provided by EEI.
Likes 0
Dislikes 0
Response
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF
Answer
Document Name
Comment
The NAGF supports preserving the language identified for deletion in Section 6 – Background and Attachment 2 – Guidelines and Technical Basis (GTB).
Likes 0
Dislikes 0
Response
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3
Answer
Document Name
Comment
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.
Likes 0
Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment
When the CIP-005 R2.4-2.5 requirements were added, entities were able to leverage existing monitoring systems and infrastructure in their High and Medium Impact Control and Data Center environments (IDS, IPS, SEIM, Intermediate Systems, etc…). Additionally, with remote Medium Impact sites, entities were already required to institute use of an Intermediate System for IRA. For assets containing Low Impact BES Cyber Systems, typically unmanned and with fewer applicable requirements, this type of infrastructure is often not in place. With the high volume of Low Impact sites, this could pose an enormous and untenable burden on RE's.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	
Document Name	

Comment
MPC has no additional comments.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	

Comment
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.

a. “Remote” would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find “3rd party” in the CIP-013 documents.

c. Where is the rest of the old “Guidelines and Technical Basis (GTB)?” We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment

SIGE would like additional clarity within the technical rationale as to whether virtual meeting sessions (e.g. such WebEx or Zoom meetings where the screen is shared, either escorted or unescorted) are considered vendor remote sessions.

Additionally, “asset” needs to be defined within the NERC Glossary of Term. “Asset” can be interpreted in many ways which may lead to inconsistent application of the requirements or definitions it is used in.

Likes 0	
Dislikes 0	

Response

Aric Root - CMS Energy - Consumers Energy Company - 4

Answer	
Document Name	

Comment
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment
Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6	
Answer	
Document Name	

Comment
Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5	
Answer	
Document Name	

Comment

Acciona Energy has no additional comments at this time, thank you for your consideration.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	
Document Name	

Comment

1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.

a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.

b. VRA needs to be limited to access to BCS.

c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale

a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.

b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents.

c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.

a. The technical rational (TR) for 6.2 states: "The obligation in Section 6.2 requires that entities which allow vendor remote access." We request updating the Requirement by adding "vendor remote access." To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase "active vendor remote access sessions". 6.1 and 6.3 do not include the word "active". Without the word 'active', 6.1 and 6.3 could include or maybe be limited to "capability" of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses “that are taking place” and the TR for 6.3 uses “active”. Sections 6.1, 6.3 and the TR should consistently use the word “active”.

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA’s. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	

Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
Vendor remote access (VRA) is not a defined term Request clarification on “malicious communications” In case there is no “vendor remote access”, which evidence is to be produced ?	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy has a higher volume of low impact locations as compared to high or mediums. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

Recommend the SDT address the term "system-to-system" by looking at CIP-002. This would greatly help industry by removing a meaningless phrase and helping industry by providing them a way to parse systems owned and used by vendors, systems owned by entity's but used by vendors, and/or systems owned and used by entities for remote access.

Recommend the SDT look at CIP-004 R4 to authorize vendors because it would align the concept of authorized vendors within the existing authorization standards and then only the systems used for access would need to be addressed in CIP-002 (recommendation 1)

Likes 0	
Dislikes 0	

Response

Michael Jang - Seattle City Light - 1

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	
Document Name	

Comment

No additional comments. AEP would like to express thanks to the standard drafting team’s hard work on this project.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	
Document Name	

Comment

Tacoma Power recommends clarifying that Attachment 2, Section 6 applies to vendor's access to low impact assets containing BES cyber systems from remote locations, as follows:

- Attachment 2, Section 6, Bullet 2: "2. Documentation of configuration of security alerts; security alerts or logging relative to activities during the **vendor remote** communication from items such as:"
- Attachment 2, Section 6: "**Vendor Remote Access:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:"

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro ackowledges the effort and hard work by SDT which went into putting together these complex changes to CIP-003-X. As identified in comments to Question 1 and 4 above, the definitions of terms and clarity of application with some specific industry use case examples will provide a clear understanding and will help to get a faster and appropriate approvals of these proposed changes.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

N&ST has reviewed the January 2020 NERC Member Representatives Committee “Policy Input Package” that preceded the February NERC Board meeting, and it is our principal observation that there was not a strong consensus among the members about the best approach to address concerns about coordinated attacks on low impact assets with vendor remote electronic access as the primary attack vector. We also noted that there were several suggestions to the effect that more comprehensive cost-benefit analyses should be performed before extending the scope of Supply Chain requirements to include low impact assets containing BES Cyber Systems.

N&ST notes the proposed requirement to require malicious communications detection at low impact assets containing BES Cyber Systems would, if effected, result in a more stringent requirement being imposed on low impact assets than on medium impact BES Cyber Systems with External Routable Connectivity at facilities other than Control Centers. N&ST is aware that the December 2091 NERC “Supply Chain Risk Assessment” raised the specter of coordinated, common mode attacks on large numbers of low impact assets, stating, “This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.” While we acknowledge this possibility and agree it is of some concern, it is our opinion that it may make more sense, and achieve a better return on investment, to add a malicious communications detection requirement for medium impact first.

It is N&ST’s opinion that introducing the concept of lower-case “interactive” vendor remote access to BES Cyber Systems at low impact assets will cause needless confusion among entities subject to requirements for upper-case Interactive Remote Access, and therefore we recommend that it be dropped. We see no need to distinguish “interactive” vendor remote access from “system-to-system” vendor remote access in CIP-003.

Likes 0	
Dislikes 0	

Response

Brian Belger - Seattle City Light - 6

Answer	
Document Name	

Comment

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

This includes systems used by vendors for system-to-system remote access and vendor "Interactive Remote Access (IRA)" (delete words in quotes) interactive remote access to low impact BES Cyber Systems.

Reasoning: The NERC defined term Interactive Remote Access includes the Electronic Security Perimeter, which is not a concept in CIP-003-8. Suggest using lowercase interactive remote access as is used in Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access section of the document.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures.

BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

Nothing additional at this time.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE has the following additional recommendations for the SDT:

- Include language for (1) software integrity and authenticity, (2) info system planning and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010.
- Include vendor multi-factor authentication (MFA). Passwords can be subjected to numerous cyber-attacks, including brute force. MFA provides an additional layer of security and protects systems should passwords become known by unauthorized users.
- Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.

Texas RE also notes that the language proposed in Attachment 1, Section 6 utilizes the undefined term “interactive” in context to vendor remote access rather than the NERC defined term Interactive Remote Access (IRA). Since the current IRA definition is associated with ESPs, Texas RE would strongly

encourage revising the IRA definition to include “assets that contain low impact BES Cyber Systems.” The definition of IRA would read: “User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s ***assets that contain low impact BES Cyber Systems***, Electronic Security Perimeter(s), or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.”

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3

Answer	
Document Name	

Comment

PNMR believes there are substatial improvements to be made to provide clarity and consistency, not only within CIP-003 but also with CIP-005

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

Attachement 2 Section 6 containes many capitalized terms that are not contained in the NERC glossary of terms. The SDT should consider not capitalizing the following terms: Security Information Management, Firewall, Intrusion Detection System, Intrusion Prevention System, Virtual Private Network, Remote Desktop, Removing, and Ethernet. By doing such the draft CIP-003-X Standard will further align with the usage of similar terms within the existing FERC approved CIP Standards.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	

Document Name	
Comment	
Please reference responses to questions 1 and 2.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The MRO NSRF has no additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Our main concern was for our market participants. The proposed addition of 6.2 for "malicious communications detection" is infrastructure dependant and could prove difficult for low impact facilities without the necessary supporting infrastructure. While we accept the reasoning for it's proposed inclusion, we would prefer "6.2 Having one or more method(s) for detecting known or suspected malicious *communications for both inbound and outbound communications, per communications capability "* *Due to the large size and scope of any implementation, in particular for the proposed 6.2 requirement of "detect malicious communications", we would prefer to see a 24 month implementation period in order to allow enough time for entities to have a full budgeting and implementation cycle.*	
Likes 0	
Dislikes 0	

Response
Martin Sidor - NRG - NRG Energy, Inc. - 6
Answer	
Document Name	
Comment
Please reference responses to questions 1 and 2.
Likes 0	
Dislikes 0	
Response
Kevin Lyons - Central Iowa Power Cooperative - 1
Answer	
Document Name	
Comment
While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. The revisions being made to CIP-003-X create more stringent controls for low impact BCS than are currently required for medium impact BCS. While this new requirement was part of the NERC study, low impact BCS should not have to meet greater requirements than higher impact level BCS. Our position is that the same revisions should be made for medium impact BCS, whether through additional work in this project or through another project. Thank you for the opportunity to comment.
Likes 0	
Dislikes 0	
Response
Richard Jackson - U.S. Bureau of Reclamation - 1,5
Answer	
Document Name	
Comment

Reclamation recommends once virtualization/zero trust architecture is implemented the SDT start focusing on incorporating low impact requirements into the other standards where applicable and change the applicable systems of the other standards to include low impact BCS.

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	
Document Name	

Comment

This Standard brings in some medium/high impact requirements for low impact. The proposed language brings in a subset of the CIP-005 requirements, which creates more stringent controls for low impact BCS than medium impact.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF

Answer	
Document Name	

Comment

We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.

Likes 1	DTE Energy, 4, ireland patricia
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	
Document Name	

Comment	
NA.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	
Document Name	
Comment	
Definitions for Vendor remote access and what constitutes malicious communications would provide some clarity and help entities determine the cost effectiveness standard. SMUD suggests changing lower case “asset” to “facility” to remove the confusion that already exists. Moving requirement 6.2 to section 3 might make it more consistent with CIP-005.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
AEPCO has signed on to the ACES comments below: We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions: While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5’s applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS	

which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS.

Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2020-03 Supply Chain Low Impact Revisions (Draft 1)
Comment Period Start Date:	8/27/2021
Comment Period End Date:	10/11/2021
Associated Ballot:	2020-03 Supply Chain Low Impact Revisions CIP-003-X IN 1 ST

There were 82 sets of responses, including comments from approximately 193 different people from approximately 128 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power, Inc.	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Chase Snuffer	Rayburn Electric Cooperative	3	Texas RE
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jodi Jensen	Western Area Power Administration - Upper Great Plains East (WAPA)	1,6	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					Bill Shultz	Southern Company Generation	5	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company -	6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Southern Company Generation		
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Cooperative		
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
Santee Cooper	Tommy Curtis	5		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA acknowledges NERC's concern regarding "aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System." [SAR, p. 1]

BPA agrees with the placement and language of CIP-003-X R1.2.6, as well as Attachment 1, Sections 6.1 and 6.3.

BPA votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium, creating confusion and implementation difficulties. BPA believes that neither the SAR nor NERC's Supply Chain Risk Assessment report* intended to require a higher bar for Low systems than already exist in M/H systems for the following reasons:

1) The Supply Chain report indicates a goal to bring Lows in line with existing M/H requirements: On p. 13 of the Supply Chain report, the summary of Q4 states that the numbers of respondents who do not apply the M/H requirements equally to their Low systems was "contrary to the expectation… that entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems." This points to an intent to copy existing M/H requirements, not add an additional requirement.

2) The SAR is inconsistent, mentioning detection of malicious communications separately from vendor access in the Purpose section, but merging them for “locations that allow vendor remote access” in the Description section.

If the SAR intended for the malicious code requirement to apply to vendor remote access, then Section 6.2 should specify “vendor remote access” to align with 6.1 and 6.3.

If the SAR intended for the malicious code requirement to apply to all remote access, then Section 6.2 belongs in CIP-003-X Attachment 1, Section 3. However, since there is no equivalent requirement for medium impact BCS, nor any projects to expand CIP-005 R1.5 to all medium impact BCS, then Section 6.2 should be removed entirely to avoid this higher requirement for low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT does not intend for low-impact sites to gain full medium/high compliance burden. The SDT agrees that the SAR uses terms that are not in the NERC Glossary of Terms. We have clarified our submissions to reduce this confusion as much as possible while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language. The SDT modified the draft language to make 6.1-6.3 consistent with intent of the SAR. The SDT sees malicious code as but one part of a remote access security landscape. Depending BES Asset configuration: leaked credentials, man-in-the-middle attacks or other cyber threats may be more of a threat, and therefore we left our wording open to an entity proportionally handling these threats themselves.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
DTE agrees with the placement and language of CIP-003-X R1.2.6 DTE votes Negative because Attachment 1, Section 6.2 introduces a higher compliance bar for Low sites than for Medium and High. Further, DTE suggests that CIP-005 R2.4 and R2.5 be modified to include the expanded scope of Low sites under applicable systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The comment of applying measures to mitigate against malicious communications being applied to Low Impact BCS and Not all Mediums has been addressed in the Technical Rationale. In addition, the SAR limited modifications to CIP-003 only.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends the SDT add the words “active,” “remote,” and “Interactive Remote Access” to Attachment 1 Sections 6 to align the language with CIP-005-6 R2 and use NERC-defined terms where possible. Section 6 should be moved and included within Attachment 1 Section 3 and not made into a new section and add “If technically feasible” to 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

From: ”Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.”

To: “Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for identifying active vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling active vendor remote access."

The phrase "determining active vendor remote access sessions" is not clear. The Technical Rationale refers more specifically to 'when sessions are initiated.

Reclamation also recommends adding "Vendor" to the NERC Glossary of Terms.

Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your response. The Team has made changes to the standard to address the issues here. We have clarified our submissions to reduce this confusion as much as possible while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language.

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity

of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT does not believe that allowing them to connect and verifying their identity is sufficient. The purpose of the SAR was to increase the security around the connection and the SDT believes that the words drafted in the standard meet the intent of the SAR. In addition, the SDT would like to point out that no time frames are specified in the draft language of proposed CIP-003-X.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
While the language addresses the risk of malicious communication, the term “system-to-system access” is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for “system-to-system access” or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has revised the drafted standard and technical rationale to remove the use of this term.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	

Answer	No
Document Name	
Comment	

The Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot.

Below are our concerns with vendor remote access and malicious communication mitigation:

The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions.

In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR?

The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration:

Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated

with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes: *6.1. Having one or more method(s) for determining vendor remote access sessions;* *6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and* *6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.*

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response
The SDT thanks you for your comment. The Team has revised the standard and technical rational to clarify the use of both of the concerning terms. In order to discuss read only access it requires a more in-depth discussion of system configurations and user account privileges. Thus the drafting team believes that the standard is drafted in a way to allow entities to address this within their individual programs.

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	

Comment
While the language addresses the risk of malicious communication, the term "system-to-system access" is ambiguous. This term has been informally discussed on several webinars and other industry forums but lacks a formal definition in the Glossary of Terms, which leads to inconsistent application throughout the industry. NRG recommends either adding a formal definition for "system-to-system access" or issuing guidance that includes only system-to-system access that either makes changes to a BES Cyber System or transfers files or data to a BES Cyber System; monitoring-only system-to-sytem remote access should be excuded.

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has revised the standard and technical rational to clarify the use of both of the concerning terms	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI believes the proposed technical requirements are reasonable and address the FERC directive; however, the technical requirements are electronic access controls. The SDT should consider including the following language in a new Attachment 1 Section 3 3.3: 3.3 Implement controls that monitor and restrict vendor remote access that: 3.3.1 Has one or more method(s) for determining vendor remote access sessions; 3.3.2 Has one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and 3.3.3 Has one or more method(s) for disabling vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT intended for section 6 to reduce confusion and focus strictly on vendor access.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No

Document Name	
Comment	
In general, Dominion Energy supports the comments by EEI. In addition, Section 6, subparts 6.1, 6.2 and 6.3 do not appear to fully align with the intended mitigations associated with the NERC Board of Trustees' Resolution dated February 6, 2020. The introduction of the requirement that includes "detecting known or suspected malicious communications" for all low impact BES Cyber Syetems is more stringent than the current requirements for monitoring communications on higher risk "medium" impact BES Cyber Systems. This more stringent requirement, by definition, lower risk assets does not appear to align with the NERC BOT intent to address the remote access risks for low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI. In addition, please see a more detailed discussion in the updated draft Technical Rationale.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
No Texas RE agrees objectives #2 and #3 have been addressed in the proposed revisions. Texas RE is concerned, however, the language proposed in Attachment 1, Section 6 does not address objective #1, "detect known or suspected malicious communications for both inbound and outbound communications". The proposed language in Attachment 1, Section 6 would require entities to "implement a process to mitigate risks associated **with vendor remote access**," including "[h]aving one or more method(s) for detecting known or suspicious malicious communications for both inbound and outbound communications." (CIP-003-X, Attachment 1, Section 6.)	

Texas RE is concerned that Section 6's focus on vendor remote access does not capture the full range of malicious communications contemplated under the low impact guidance documents. In the event of a supply chain attack, malicious communications can occur whether or not a Responsible Entity has established an authorized channel for vendor communications. Additionally, in the event of a supply chain attack, malicious communications, such as compromised Cyber Assets attempting to communicate with a Command and Control server, can occur at locations where the Responsible Entity has deliberately not established channels for vendor remote access.

Based on this perspective, therefore, Texas RE recommends that the SDT clarify that CIP-003 low impact monitoring obligations extend to **all** inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of vendor remote access. Texas RE recommends moving the proposed language in Attachment 1, Section 6.2 to Section 3 (Electronic Access Controls) so it is clear malicious communication monitoring and detection method obligations apply to all communications, not simply vendor remote access communications.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
Malicious communications is not required at all medium impact BCS. It is only required to detect malicious communications at medium impact BCS at Control Centers. It is unreasonable to have low impact requirements that are more stringent than some medium impact. The measures section in Attachment 2 provides great examples; however, the measures go above and beyond some medium impact requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Suggest interchanging the order of 6.2 and 6.3. 6.2 as is not specific to vendor remote access and it would be clearer to understand the security objectives. To ensure even less confussion consider moving 6.2 to Section 3. The SARs scope of '(1) detect known or suspected	

malicious communications for both inbound and outbound communications' is not specific to only vendor remote access, but all routable protocol.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to change the order of 6.2 and 6.3. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

The language proposed in CIP-003-X Attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- Context and usage of the term 'malicious communication' needs clarity and BC Hydro proposes to add a definition of the term 'malicious communication' in "NERC glossary of terms" to support the understanding
- Similarly BC Hydro proposes defining and adding term 'vendor remote access' to NERC glossary of terms
- Who and what is considered a 'vendor' also need to be defined in the glossary of terms for clarity and understanding
- The language used in Section 6.2 is referring to 'known or suspected malicious communications'. The use of word 'suspected' is quite open with respect to application and usage. Entities may have varied understanding and consideration of what is suspected and what is not. BC Hydro recommends adding clarity and provide examples of use cases and applicability to improve understanding and to better scope the requirements.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.2 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.2 does offer possible mitigation of the risks i.e.,

'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.2 completely.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT does not intend for low-impact sites to gain full medium/high compliance burden. The SDT agrees that the SAR uses terms that are not in the NERC Glossary of Terms. We have clarified our submissions to reduce this confusion, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language. The SDT modified the draft language to make 6.1-6.3 consistent with intent of the SAR. The SDT sees malicious code as but one part of a remote access security landscape. Depending BES Asset configuration: leaked credentials, man-in-the-middle attacks or other cyber threats may be more of a threat, and therefore we left our wording open to an entity proportionally handling these threats themselves	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power does not agree with the proposed language and suggests the following edits: • Attachment 1, Section 6, replace the high level Section 6 language with "Section 6: **Vendor remote access**: Each Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:" • Attachment 1, Section 6, Bullet 6.2, "Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and"	

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT does not intend for low-impact sites to gain full medium/high compliance burden. The SDT agrees that the SAR uses terms that are not in the NERC Glossary of Terms. We have clarified our submissions to reduce this confusion, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language. The SDT modified the draft language to make 6.1-6.3 consistent with intent of the SAR. The SDT sees malicious code as but one part of a remote access security landscape. Depending BES Asset configuration: leaked credentials, man-in-the-middle attacks or other cyber threats may be more of a threat, and therefore we left our wording open to an entity proportionally handling these threats themselves

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees with the overall sentiment of the proposed language in Attachment 1 Section 6, we believe it could be modified to provide a more clear understanding of how Responsible Entities are expected to comply. AEP recommends that additional language be included to specify that Section 6 subparts are only applicable to Entities that have implemented vendor remote access as part of their business process. Please see recommendations for language below.

Section 6: Vendor remote access: For low impact BES Cyber System(s) identified pursuant to CIP-002, Responsible Enties that have implemented vendor remote access shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) that include:

6.1 Having one or more method(s) for determining when vendor remote access sessions have been initiated;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and *6.3 Having one or more method(s) for disabling vendor remote access.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Malicious communications (whatever that means) has no bearing on access and was not part of the NERC Low Impact report so why is it in this draft? If NERC wishes to address malicous code, it should do it in Systems Administration. We do not support the use of meaningless phrases such as malicious communications to meet security objectives for compliance. There is a tendency to re-use these phrases by SDT's in an effort to seemingly make it easier to use them because they exist in other areas of the standards however that propoagates a continual mantra of applying something that could mean anything to anyone. Why not just use language for what we are trying to acheive? Another meaningless phrases is system-to-system.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response. The SDT has clarified our submissions to reduce this confusion, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy supports EEI comments. Additional analysis would be needed to review the data diode configurations at low impact locations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI. The drafting team asserts that analysis on security configurations is a responsibility of the entity and the method to comply can be addressed in the entities plan.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Becky Webb - Exelon - 6	
Answer	No
Document Name	

Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy does not agree with the language proposed in Attachment 1 Section 6. Vendor remote access is not a defined term. For this to be an effective requirement this term needs to either be defined in the NERC Glossary of Terms, defined within Attachment 1 Section 6 or a term that is defined in the NERC Glossary of Terms should be used in lieu of it, such as Interactive Remote Access (Please note IRA definition would require modification to apply to low impact). If the Standards Drafting Team (SDT) were to define vendor remote access, Acciona Energy would suggestion the following definition: Vendor Remote Access (VRA): Access by a vendor(s) of the Responsible Entity from a Cyber Asset outside the asset containing low impact BES Cyber System(s) that permits remote commands, control functions, software changes or firmware changes (e.g. 'write permissions') of BES Cyber Assets of the low impact BES Cyber System(s). Using the aforementioned definition for VRA, Acciona Energy would suggest the following Section 6 language:	

Section 6: Vendor Remote Access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with Vendor Remote Access to low impact BES Cyber Systems that includes: 6.1 Having one or more method(s) for determining Vendor Remote Access sessions; 6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound Vendor Remote Access communications; and 6.3 Having one or more method(s) for disabling Vendor Remote Access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment and your efforts to help clarify the language. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	

Answer	No
Document Name	
Comment	
MPC supports MRO NERC Standards Review Forum comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to MRO NERC Standards Review Forum.	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
It is difficult to determine if the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems without first defining what “vendor remote access” is. The use of the undefined term “vendor remote access” in CIP-003-9 will cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. The term "malicious communications" should be defined. Is this known malware or does it include any communications to or from an unknown ip address? Would we get penalized for not recognizing a zero day attack? The term "session" should be defined (and maybe "remote session" as well). Is this an active session or any session that is currently defined but inactive (as in through established firewall rules). Could we be penalized for not disabling inactive sessions in the event of an attack?	
Likes 0	

Dislikes 0	

Response
Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	

Comment
The NAGF recommends the following additions (**Bold**) to Attachment 1 Section 6, aligning the proposed language with the NERC Board resolution and CIP-005 R2.4 of the NERC Reliability Standards: *Section 6: Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with **active** vendor remote access (including **Interactive Remote Access** and system-to-system **remote** access) to low impact BES Cyber Systems that includes:* *6.1 Having one or more method(s) for determining **active** vendor remote access sessions;* *6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and* *6.3 Having one or more method(s) for disabling **active** vendor remote access.*

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms.

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, APPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board	

resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA agrees with several other utility comments that the proposed language is more stringent and not consistent with NERC CIP High and Medium Assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment. Please see the response to EEI's comment.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, FMPA does not agree that the language meets what is specified in the NERC Board Resolution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The NERC Board Resolution recommends that malicious communication and vendor remote access be dealt with individually rather than together as is done in the proposed standard revisions. Therefore, OUC does not agree that the language meets what is specified in the NERC Board Resolution.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern supports the comments submitted by EEI. In addition, we note Section 6 requires implementation of a process for all assets containing low impact BCS even if no such vendor remote access capability exists. In these instances, it requires methods to determine, detect, and disable a non-existent capability. We suggest the process and implementation of it be made conditional upon such access existing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
MISO supports the comments of the Midwest Reliability Organization NERC Standards Review Forum (MRO NSRF) and thanks the Standard Drafting Team (SDT) for their work in drafting language in response to the NERC Board of Trustees (BOT) recommendations and approved Standards Authorization Request (SAR). While the MRO NSRF have some concerns with the proposed language, we agree with the general purpose of Project 2020-03 - Supply Chain Low Impact Revisions. The MRO NSRF acknowledges that a vendor remotely accessing low impact BES Cyber Systems poses security risks to the Bulk Electric System (BES) that must be mitigated. We feel that this first posting is very close to a final acceptable product and addressing our concerns with clarification of verbiage around a vendor's remote access and in detecting known or suspicious malicious communications will result in passing the next ballot. Below are our concerns with vendor remote access and malicious communication mitigation: The MRO NSRF has concerns with the use of the undefined term 'vendor remote access'. The use of this term or phrase continues to cause inconsistencies with interpretation across regions that often results in over-reach or misinterpretation that read only information sharing somehow constitutes access. The phrase 'vendor remote access' should be clarified and either be in the NERC Glossary of Terms, Implementation Guidance, Technical Rationale, or addressed in a CMEP Practice Guide. The SDT could also choose to rephrase the language in way that would exclude read-only sessions. In Section 6 the SDT chose to include language "including interactive and system-to-system access." While the MRO NSRF understands the drafting team took language from CIP-005 R2.4 to maintain consistency, this also increased the scope from what was stated in both the SAR and NERC BOT recommendations. Was it the SDT's intention to do this and is it allowed within the scope of the approved SAR? The MRO NSRF offers the following suggestion for requirement language for the SDT's consideration: Attachment 1 Section 6 – Vendor Communications with BES Cyber Systems *Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS for assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions (including software updates) of low impact BES Cyber Systems that includes:* *6.1. Having one or more method(s) for determining vendor remote access sessions;*

6.2. Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications as vendor remote access sessions are occurring; and *6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to MRO NSRF.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form (FINAL).docx
Comment	
The applicable resolution calls for additional levels of protection; however, the proposed language places an unduly high burden for low impact locations from a cost-effectiveness perspective. In particular, the proposed language effectively requires that the level of protection for low impact assets be effectively equivalent to the level of protection required to be applied to medium-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a larger discussion in the updated draft technical rationale.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No

Document Name	
Comment	
OKGE supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E agrees with the comments provided by the Edison Electric Institute (EEI) related to the use of the wording "vendor remote access". Either make this a term in the NERC Glossary or modify Section 6 as indicted in the EEI comments to help in consistency across the industry.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to clarify the use of the terms vendor remote access. Please see SDT response to EEI comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No

Document Name	
Comment	

To clarify and remove ambiguity associated with the BOT recommendations, the term "vendor remote access" should be defined in the NERC Glossary rather than in an attachment to a Standard. Defining "vendor remote access" will ensure registered entities have a consistent understanding of the term in this and other Standards that may use the term.

As an alternative to defining "vendor remote access" in Section 6, EEI offers the following for consideration.

Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: *For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:*

*6.1 Having one or more method(s) for determining **when** vendor remote access sessions **have been initiated**;*

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications:

*6.3 Having one or more method(s) for disabling **active** vendor remote access **when necessary.***

In addition to the above comments, the proposed language in Section 6, part 6.2 is understood to add new requirements that appear to obligate entities to install IDS-like solutions for low impact BCS which is a higher bar than what is currently required for EAPs at Medium impact BCS with ERC. While it is unclear whether this was the NERC BOT's intent, such a requirement raises questions about CIP-005-6, Requirement R1, subpart 1.5.

Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to remove the use of the terms vendor remote access. The SDT has address scope of Section 6.2 for malicious communications in the updated draft Technical Rationale. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response, specifically the idea of limiting the requirement to Interactive Remote Access	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State would like to see a definition of vendor remote access either in the Glossary of Terms, Technical Rationale or in the other guides such as the Implementation or the CMEP guides. There is too much misinterpretation surrounding vendor remote access. Tri-State also recommends adding additional language to the term system-to-system to eliminate ambiguity. Proposed language would read ("including interactive and system-to-system **with command-and-control capability access**) ...	

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to clarify the use of the terms vendor remote access. We have clarified our submissions to reduce this confusion, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language.

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD agrees that the proposed language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems, but believes that it would create less confusion for industry if the a “low impact asset” was referred to as a “low impact facility.” Using lower case asset versus upper case Asset has been a source of confusion since the low impact standards became effective.

SMUD does not believe that CIP-003 R2 Section 6 Part 6.2 belongs in section 6. This requirement may be better suited for Section 3, but should be changed to clearly reflect that the applicability is to vendor remote access (which is not in the current wording as part of Part 6.2). At a minimum, SMUD recommends changing the wording in Part 6.2: e.g.

“6.2 For vendor remote access, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and….”

Regional Entities could potentially interpret 6.2 to increase the scope to have one or more methods for detecting any malicious communications. This could increase the cost to implement and burden of proof to demonstrate compliance. SMUD would suggest adding “vendor remote access” to the requirement so that the scope is absolutely clear.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

The SDT thanks you for your comments. The team has revised the drafted standard and technical rationale to address location of Section 6.2. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. For this reason Section 6 is being kept to limit scope appropriately.

Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	

Comment

: It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the SDT response to question 6.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
PNMR does not agree with industry partners and their recommendation to define "vendor remote access" within the requirements. This definition should be left to the utility.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence:

{C}1.) Revise 6.1 to read: "Having one or more method(s) for determining when vendor remote access sessions have been initiated;"

{C}2.) Revise 6.3 to read: "Having one or more method(s) for disabling active vendor remote access when necessary."

{C}3.) Remove the Section 6 parenthetical "(including interactive and system-to-system)" as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets.

Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, "This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems" be revised to "This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access." Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to address these concerns.

Brian Belger - Seattle City Light - 6

Answer	Yes
Document Name	

Comment

Yes, however, the use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term "vendor". Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users

are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments. As for part one of your comments, the SDT has revised the drafted standard and technical rationale to clarify the use of this term. As for part two of your comments, The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
While N&ST agrees the proposed Section 6 requirements align well with the Board's 3-part resolution, N&ST believes they lack sufficient precision and clarity (e.g., would they apply to ANY vendor remote access to assets containing low impact BES Cyber Systems or only to those subject to "Electronic Access Controls" defined in CIP-003-8, Attachment 1, Section 3?).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the scope is clearly defined as only pertaining to BES Cyber Systems in parent Requirement R2 as well as throughout Attachment 1. Additionally, the SDT has revised the drafted standard and technical rationale to address this concern.	

Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	

The use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term "vendor". Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments. As for part one of your comments, the SDT has revised the drafted standard and technical rationale to clarify the use of this term. As for part two of your comments, The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written it increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with the adequacy of implementing and auditing. See the response to question 6 for more details.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see SDT response to question 6.	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Indiana Electric (SIGE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments.	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Yes, however, the use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for: Attachment 1 Section 6: Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks	

associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for initiating and disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

Additionally, regarding 6.2, while it is a good idea and certainly supports risk management of vendor remote access, this seems outside the scope of the vendor remote access section. Including it here implies that we should detect known or suspected malicious communications only within the context of vendor remote access sessions. To be more clear, we would suggest moving this sub requirement from 6.2 to instead become 3.3 within the electronic access controls section.

Moreover, there is a need to further clarify and define the term "vendor". Does this exclude contractors and consultants?

There is no need to single out vendors when discussing remote access for whatever purpose. Any remote access, whether it be vendor, contractor, consultant, employee, engineer, programmer – they are all users employing remote access and as such, should be subject to security controls contemplated and spelled out in Attachment 1, Section 3 without having to be spelled out in minute detail. Although this section was designed for Supply Side Security, it could simply state that vendors are also subject to all security controls that other users are subject to when it comes to remote access. As such, preventive and corrective security controls/measures taken by the entity apply to them as well.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comments. As for part one of your comments, the SDT has revised the drafted standard and technical rationale to clarify the use of this term. As for part two of your comments, The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain

report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence: 1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;” 2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.” 3.) Remove the Section 6 parenthetical “(including interactive and system-to-system)” as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets. 4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to address these concerns.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric (CEHE) agrees the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE thanks the SDT for their work on this project, and commends the team on their fidelity to the SAR. BHE agrees the language proposed in Attachment 1 Section 6 satisfies the NERC Board resolution, but proposes the following recommendations to maximize congruence: 1.) Revise 6.1 to read: “Having one or more method(s) for determining when vendor remote access sessions have been initiated;” 2.) Revise 6.3 to read: “Having one or more method(s) for disabling active vendor remote access when necessary.”	

3.) Remove the Section 6 parenthetical "(including interactive and system-to-system)" as it was not mentioned in the resolution, and could imply the same level of required protection as called for in CIP-005-7 R2.4 and R2.5, which may not be justified for low impact assets. 4.) Instead, please address within the technical rationale document, Rationale Section 6 of Attachment 1, the intended scope of vendor remote access with respect to vendor read-only access for both system-to-system and interactive access. BHE proposes the last sentence, "This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems" be revised to "This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access." Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comments. The SDT has revised the drafted standard and technical rationale to address these concerns.

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment
Yes, however, the requirements for malicious communications at low impact are similar to that which already exists in the current enforceable versions of CIP-005-6 Requirement R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for High impact BES Cyber Systems (BCS) and EAPs for Medium impact BCS at Control Centers. The existing CIP-005-6 requirement do not apply to Medium Impact BCS with External Routable Connectivity (ERC). Was it the 2020-03 SDT's intention for this draft of the proposed low impact requirements for malicious communication to impose IDS-like solutions for low impact that are in fact a higher bar than what would currently be required for EAPs at Medium impact BCS with ERC?

Also, the use of the undefined term 'vendor remote access' continues to cause inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, "***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes: 6.1 Having one or more method(s) for determining vendor remote access sessions; 6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and 6.3 Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS."***	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. For the first comment, please see a more detailed discussion in the updated draft Technical Rationale that addresses this concern. For the second comment, the SDT has revised the drafted standard and technical rationale to clarify the use of this term. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with adequacy of implementing and auditing. See response to question 6 for more details.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. See the SDT response for Question 6	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Although the language addresses the NERC Board resolution, it goes too far placing compliance burden beyond requirements established for high and medium impact. Low impact requirements should match the reliability risk. This problem begins in Requirement R1. For medium and high impact, this point is covered by the defined term Interactive Remote Access which clearly defines “remote access” and includes both vendor and Responsible Entity. For low impact, “vendor remote access” is not defined and allows too much audit subjective interpretation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	

Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations?	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Vendor remote access can be confused with vendor access via Transient Cyber Asset connected to the Responsible Entity's local network to "remotely" connect to an asset containing low impact BES Cyber Systems (behind physical security controls). "Vendor remote access" must be defined to remove all subjective audit interpretation. Suggest the following: Vendor remote access: for remote routable protocol access originating outside the Responsible Entity's physical security controls for assets containing low impact BES Cyber System via an Internet Service Provider (ISP) from Cyber Assets used or owned by vendors, contractors or consultants…	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT does not see overlap between TCA access controls and Vendor remote access in the proposed draft language.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	

The lack of definition or clarification of the word “remote” might create confusion, please consider adding a definition, either in the NERC Glossary or a standard-specific definition.

The phrase “interactive access” is also confusing and should be further defined/clarified within this document, or a different phrase should be used.

Additionally, the term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This makes it appear that the Low Impact requirement is more stringent than the higher impact levels.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3.

Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator? Suggest that language be included to specify that remote means physically external to the site to be consistent with the CIP Low Impact protection framework and requirements for communications.

Request consistent use of “Low Impact” or “low impact.”

The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI’s comment.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Needs to be further clarified	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CEHE does not agree Attachment 1 Section 6 only addresses a vendor's access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3, which could allow an interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not.

Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5, which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.

LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman

Answer	No
Document Name	

Comment

The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses

vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Hao Li - Seattle City Light - 4	
Answer	No
Document Name	
Comment	

: No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The Board Resolution recommends 3 projects to be revised in the standard with respect to policies for low impact BES Cyber Systems, the second of which is to determine with active vendor remote access sessions are initiated. So it is not clear that Section 6 only addresses vendor access to low impact assets. It appears to also address malicious communications and disabling vendor remote access which the Board Resolution suggests should be dealt with in separate revisions.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	

Comment
In 6.1 we are required to have "...one or more method(s) for determining vendor remote access sessions." Determining what about them? that they are active or that they merely exist, whether or not they are active. In 6.2 I don't see the benefit of monitoring outbound communications for malicious communications when those communications are only outbound, as with a data diode. the only reason I can think of to monitor outbound communications is as an indicator of response to a remote command & control server. That would only make sense in a two-way communication. In 6.3 I believe that "...disabling vendor remote access" could be interpreted as disabling ALL vendor remote access if any remote access is seen to have malicious communications. If there are multiple sessions ongoing to multiple vendors (as well as employees) we could be found in violation for not shutting down all vendor sessions upon learning that one session is suspicious. In addition we would have to be able to determine which sessions are vendors in order to avoid shutting down employee sessions. Either that or just shut them all down. There is no mention of notifications or timeframe here. Sessions must be monitored but it follows that unless someone is notified in a timely fashion of malicious communications, nothing can be done in a reasonable period of time. And what is a reasonable period of time? A minute, an hour, a day? If we use logging as a method of monitoring, would a daily check of the logs be sufficient. I think we're at the mercy of the auditor on this but those with CIP-005 experience may have a better feel for how this could be implemented and what an auditor might expect.

Likes 0	
Dislikes 0	

Response
Thank you for your comments asking to clarify active vendor remotes access. The Drafting team has discussed the phrase “active vendor remotes access” at great length. The intent has been to identify when a vendor is interacting with an entity’s system. The interaction would include updating their hardware, software, or having the ability to modify, operate or manipulate the system and affect the BES as part of their support. The team has strived to honor the various business practices by not placing time frames, or times for detection and disconnection requirements to respect each entity’s processes, the related risk, and the technologies applied. In addition, the Drafting

team has removed the term “active” in an attempt to reduce confusion that the term added, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The SDT has not defined “Vendor” to date. Without “vendor” being defined it is difficult to tell who would be in scope and required to adhere to Attachment 1 Section 6. This is also problematic in regards to Supply Chain for Medium Impact and High impact BES Cyber Systems. We would suggest defining “vendor”.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT has clarified our submissions to reduce this confusion, while also working within the bounds of the SAR, existing NERC Glossary Terms and existing standards language.	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree Attachment 1 Section 6 only addresses vendor’s access to low impact assets containing BES Cyber Systems. Part 6.2 does not explicitly refer to vendor remote access sessions similarly to Parts 6.1 and 6.3 which could allow interpretation that having one or more method for detecting known or suspected malicious communications for both inbound and outbound communications should be applied broadly to all low impact assets, regardless of whether vendor remote access sessions are permitted or not.	

Furthermore, Part 6.2 is worded similarly to CIP-005 R1 Part 1.5 which is applicable to Electronic Access Points (EAPs) for high impact BES Cyber Systems and EAPs for medium impact BES Cyber Systems at Control Centers. The proposed 6.2 as worded would imply that Electronic Security Perimeters (ESPs) and EAPs are required for all low impact BES Cyber Systems, which would also exceed the requirements for medium impact BES Cyber Systems since CIP-005 R1 Part 1.5 is only applicable at medium impact BES Cyber Systems at Control Centers and is not applicable to generation resources or transmission substations.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow the use of CIP-003-8, reference model 3. Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator? Request consistent use of “Low Impact” or “low impact.”	

The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	No

Document Name	
Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
To ensure complete clarity, Acciona Energy suggests using a defined term, please see Acciona Energy's answer to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	

Answer	No
Document Name	
Comment	
Request clarification on “remote” since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. “Remote” could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow use of CIP-003-8, reference model 3. Request clarification on “remote location.” The question includes “remote location” which is not defined. Is the generation switch yard a different location than the generator? Request consistent use of “Low Impact” or “low impact.” The term “mitigate” in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term “mitigate” in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Request clarification on “remote location” with respect to BCS	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The terminology of low impact BES cyber systems versus low impact assets needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the scope is clearly defined as only pertaining to BES Cyber Systems in parent Requirement R2 as well as throughout Attachment 1. Additionally, the SDT has revised the drafted standard and technical rationale to address this concern.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
It includes malicious communications which has nothing to do with access.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, clarifying changes have been made to the standard and technical rationale.	
Michael Jang - Seattle City Light - 1	
Answer	No
Document Name	
Comment	
Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power does not agree that the proposed language clearly addresses vendor’s access to low impact assets containing cyber systems from remote locations. Tacoma Power suggests the following edit to Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”	

Tacoma Power is also concerned that Bullet 6.2 institutes more stringent requirements for low impact BCS at substations or generation units than what is currently required under CIP-005 for similar medium impact assets. The requirement in CIP-003-X should be limited to detection of malicious communications for assets at control centers, in alignment with the scope of CIP-005.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As mentioned in comments related to Question 1 above, 'vendor remote access' needs clarity of understanding and clear definitions of the terms for appropriate applicability.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST believes the proposed Section needs to be clear about whether or not it applies only to BES assets containing low impact BES Cyber Systems that are subject to “Electronic Access Controls” defined in CIP-003-8, Attachment 1, Section 3.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Brian Belger - Seattle City Light - 6	
Answer	No
Document Name	
Comment	
No. Unless the section 6 is revised with the redefined “Vendor Remote Access” in the comments of #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	

Consider not using ‘a process’ in CIP-003, which is consistent with other Sections of CIP-003. The first part of Attachement 1 speaks to having plan(s). Also suggest using ‘electronic access controls’ as used in other Sections or just ‘controls.’ Consider the following edits for clarification:

“Section 6: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002 that permit active vendor remote access to low impact BES Cyber Systems, the Responsible Entity shall implement electronic access controls to mitigate risks associated with active vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:”

To be consistent with the language of the SAR and CIP-005-6, consider using ‘active vendor remote access’ and not just ‘vendor remote access’ in Section 6, 6.1 and 6.3. From a technical basis it is not clear what would the difference be between the two uses.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
The way the 6.2 is written it appears that all communications must be monitored for malicious communication. It is not apparent that the malicious communications requirement only applies to situations where vendor remote access is allowed. This is only present in the technical rationale document, and it should be more clearly stated in CIP-003-X Attachment 1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	
CIP-003 Section 6.2 requirement seems to establish a higher bar than the similar requirement in CIP-005 R1.5 for MIBCS at Control Centers. Additionally, CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low	

impact BES Cyber Systems". Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Regarding the concern that the draft language established a higher bar than similar requirements in CIP-005, clarifying changes have been made to the standard and technical rationale to address this concern. The use of the language was to ensure that industry understood that the Team was scoping this requirement to focus on low impact BES cyber systems.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference "remote locations".	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO supports the NPCC submitted comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NPCC.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
In Attachment 1, Section 6, it is clear that the section is addressing vendor access to low impact assets containing BES cyber systems. However, it is not clear that the access is from remote geographical locations or from outside the point where electronic communication is controlled. Nowhere in Section 6 does it reference “remote locations”.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team has made clarifying changes to the standard to address these concerns.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Attachment 1, Sections 6.1 and 6.3 clearly specify that they apply to vendor access. BPA does not believe Section 6.2 provides the same clarity.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	

Comment	
The language in Attachment 1, Section 6.2 – Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications is too broad if it is meant to only cover malicious communications relating to vendor remote access.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees to the language in Section 6 only addresses vendor access to low impact assets containing BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
It is clear Section 6 only addresses vendor's access to assets containing low impact BES Cyber Systems from remote locations. However, in conjunction with EEI comments on Q1 further clarity on both 'remote' and 'access' is needed. For example, is data from an entity's BCS that is directed through a data diode to physically enforce an outbound only connection to a vendor system included in 'system-to-system vendor remote access'?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI in question 1.	

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Becky Webb - Exelon - 6	
Answer	Yes

Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Yes, but for additional clarity BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity's network is not considered vendor remote access.	

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	

Response

Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD would like to see more clarity regarding what constitutes a vendor. If an entity has contracted with an orgization to operate an asset, are all communications and connections from outside of the asset considered vendor remote access? There are use cases where the entity may contract the operation of an asset that the entity itself has no access to.

Would a contractor, issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor?

The two examples provided are use cases that SMUD feels should not be left up to the region entities.

Likes 2	Platte River Power Authority, 5, Archie Tyson; DTE Energy, 4, ireland patricia
Dislikes 0	

Response

Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale. The responsible entity assumes compliance obligation based on their registration and the NERC Rules of Procedure.

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO Supports the NPCC Submitted comments	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see response to NPCC comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
In general, Dominion Energy supports the comments from EEI. In addition, Dominion Energy is concerned that when reviewing Attachment 1, Section 6 the current language appears to broaden the scope of applicability to any asset containing the low impact BES Cyber Systems rather than just to the low impact BES Cyber System itself. The language should be clarified to enure that the scope is limitied to just the cyber system and not the entire asset.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see respond to EEI. The SDT believes that the scope is clearly defined as only pertaining to BES Cyber Systems in parent Requirement R2 as well as throughout Attachment 1. Additionally, the SDT has revised the drafted standard and technical rationale to address this concern.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Current low impact BCS do not include or required IDS/IPS. The proposed revisions seem to expand the need for them.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, The SDT has addressed this issue within the Technical Rationale.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
Current low impact BCS do not include or require IDS/IPS. The proposed revisions seem to expand the need for them.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, The SDT has addressed this issue within the Technical Rationale.	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and”

For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed.

Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language.

CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC

Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan, and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language. CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan, and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The language in Sections 6.1-6.3 applies to assets that contain BES Cyber Systems. This potentially draws in remote access to non-CIP devices that are located within that asset. The language should be updated to specifically point to the BES Cyber System within the low impact asset. This is different than the way that CIP-003 is written and may need a different Requirement to address.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the scope is clearly defined as only pertaining to BES Cyber Systems in parent Requirement R2 as well as throughout Attachment 1.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

We agree with and support EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC agrees with the EEI Comment Form response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see the response to EEI's comment.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Section 6 includes "vendor remote access" which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include "vendor remote access". This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.	

Recommend adding “vendor remote access sessions” to 6.2. For example “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and” For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed. Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – “Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers.” Another possibility is to leverage CIP-003 Section 3 “Electronic Access Control” scoping / boundary language. CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5’s Requirement but R1.5 is applicable to High Impact EAP’s and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5’s Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan, and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No

Document Name	
Comment	
Section 6 includes “vendor remote access” which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include “vendor remote access”. This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3. Recommend adding “vendor remote access sessions” to 6.2. For example, “Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and”{C}{C}	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Clarifying changes have been made to the standard and technical rationale.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Language exceeds medium and high impact by not exempting low impact BES cyber systems not having External Routable Communication. This increases scope.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT has made changes in the proposed draft language to address this concern.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
CIP-003 R2 requirement establishes the applicability to “at least one asset identified in CIP-002 containing low impact BES Cyber Systems”. Why is it necessary to restate applicability in CIP-003 R2, Att1, Sec 6. Usage of this statement is inconsistently used through CIP-003 R2, Att1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The use of the language was to ensure that industry understood that the Team was scoping this requirement to focus on low impact BES cyber systems.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
While it does limit the scope to low impact BES cyber systems, it does not limit the scope to only those **assets** containing low impact BES cyber systems that permit vendor remote access.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT asserts that entities that do not allow vendor electronic access will have that written into their plan and the drafting team believes that each entity needs to consider their unique security environment when creating their plan in order to comply.	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	

However, the use of the term 'vendor remote access' continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS.

We also request consideration of alternative language in the parent requirement such as: Requirement "**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**".

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
Michael Jang - Seattle City Light - 1	
Answer	Yes
Document Name	
Comment	

The use of the term 'vendor remote access' continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for:

Attachment 1 Section 6:,

Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:

6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;

6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and

6.3. Having one or more method(s) for disabling a vendor's ability to remotely perform command and control functions of the low impact BCS. We also request consideration of alternative language in the parent requirement such as: Requirement "***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
It does because CIP-003 is applicable only to Low Impact assets (not Cyber Systems)	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
The language implies that additional analysis is required for vendor remote access once an analysis was performed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team is not clear on the additional analysis that is being referenced. Please provide additional details in the second comment form if the concern is not addressed in the second proposed draft standard.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see our response to EEI comment.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see our response to EEI comment.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see our response to EEI comment.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment. Please see our response to EEI comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Yes, NERC Reliability Standard CIP-003-8, Attachment 1 is only applicable to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees the language in Attachement 1 Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
APPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the drafted standard and technical rationale to clarify the use of the terms vendor remote access, however the intent of the project is to address low impact BES Cyber Systems.	
Hao Li - Seattle City Light - 4	
Answer	Yes

Document Name	
Comment	
However, the use of the term ‘vendor remote access’ continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term ‘vendor remote access’ appears outside the scope of the 2020-03 SAR, we request consideration of alternative phrasing like but not limited to the following for: **Attachment 1 Section 6:,** ***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact BES Cyber Systems that includes:*** ***6.1. Having one or more method(s) for determining and monitoring vendor remote access sessions;*** ***6.2. Having one or more method(s) for detecting and mitigating known or suspected malicious communications for both inbound and outbound communications; and*** ***6.3. Having one or more method(s) for disabling a vendor’s ability to remotely perform command and control functions of the low impact BCS.*** We also request consideration of alternative language in the parent requirement such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
FMPA suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has revised the drafted standard and technical rationale to clarify the use of the terms vendor remote access, however the intent of the project is to address low impact BES Cyber Systems.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
OUC suggests deleting the lead-in of, “Vendor remote access: .” Otherwise, the first clause of the sentence in Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT has revised the drafted standard and technical rationale to clarify the use of the terms vendor remote access, however the intent of the project is to address low impact BES Cyber Systems.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern believes the language in CIP-003 R2 makes it clear that all sections in Attachment 1 are limited in scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes the language of Section 6 limits the scope to low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
However, the use of the term 'vendor remote access' continues to affect the scope and create inconsistencies with interpretation across regions, and over-reach or misinterpretation that read only information sharing somehow constitutes access. Given defining the term 'vendor remote access' appears outside the scope of the 2020-03 SAR, ATC requests consideration of alternative phrasing like but not limited to the following for Attachment 1 Section 6:, "***Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic access that permits a vendor to perform remote command and control functions of low impact***	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team asserts that clarifying changes were made in the draft standard to address confusion around terms that are not defined in the NERC Glossary of Terms. The SDT does not believe that only providing protections from vendor performing remote command and control functions eliminates the risk posed by malicious communications.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant

Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cost can vary widely depending on interpretation of vague language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT understands that there may be technology and procedural costs associated with the proposed draft standard.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
At this point, we believe the framework still requires significant modifications before assessing the cost effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC does not agree with the EEI response. ITC believes that this requirement is NOT as cost effective and would require specialized equipment and/or processes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands that there may be technology and procedural costs associated with the proposed draft standard.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional consideration needs to be given to the Virtualization project and flexibility that access approach can allow	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the standard as drafted is technology agnostic.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
At this time PG&E does not have information to determine if the modifications are a cost-effective approach. PG&E would have preferred to answer this as un-known and not "No", but that option does not exist within the NERC Standards Balloting and Commenting System (SBS).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT will take this suggestion back to the NERC standards staff.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Due to the number of assets potentially affected by the proposed changes as well as the complexity of the proposed measures, implementation of proposed language would be disproportionately costly to implement given the risks associated with low-impact assets. GSOC proposes that the standard revision include qualifications similar to those on the medium-impact assets such as limiting the scope to those assets with External Routable Connectivity as well as explicitly limiting the scope to routable protocols	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see a more detailed discussion in the updated draft Technical Rationale.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports the comments submitted by the MRO NSRF and does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	
BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA does not agree it's cost effective for Low Impact Assets to be subjective to more stringent requirements than NERC CIP High and Medium impact Assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply. Please see a more detailed discussion in the updated draft Technical Rationale.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The cost and implementation could be quite significant if entities were to have to renegotiate contracts and put in place remote vendor access controls for remote low-impact facilities The cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply. Please see a more detailed discussion in the updated draft Technical Rationale.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Low impact environments are often unmanned and lack the types of infrastructure required for determining, detecting, and disabling malicious activity (IDS, IPS, SEIM, Intermediate Systems, etc…). These new requirements could potentially expand the scope of existing low impact programs with respect to cost for new monitoring functionality.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	
MPC supports MRO NERC Standards Review Forum comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NERC Standards Review Forum comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team agrees that monitoring communication at Low Impact BES Cyber Systems is the intent, but it is focused on vendor access.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy does not believe that the modifications will be cost effective within the current scope of the implementation plan. The cost of deploying security measures to meet the requirements within an 18 month time frame at hundreds of low impact substations and other	

assets will be a strain on entities budgets and existing IT/OT security personnel. Evergy suggests spreading this effort out across a longer time frame of 36 months or more to be less impactful financially and more realistically achievable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team agrees that monitoring communication at Low Impact BES Cyber Systems is the intent, but it is focused on vendor access.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Many entity's will believe that "malicious communications" translates to Intrusion Detection Systems for Low Impact assets. That could translate to $millions for entity's.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see discussion about IDS/IPS in the technical rationale.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

Tacoma Power recommends editing the language in Attachment 1, Section 6, Bullet 6.2 in order to provide a more cost effective approach. Instead of detecting, Tacoma Power proposes changing the measure to monitoring for malicious vendor remote access communication, as follows: Attachment 1, Section 6, Bullet 6.2, “Having one or more method(s) for **monitoring** known or suspected malicious **vendor remote** communications for both inbound and outbound communications; and”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the draft proposed language is in line with the language in the SAR.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Although the cost may differ between entities, it's impact may change based on understanding & clarity of terms and scope of application. As advised in comments of Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However requirement in CIP-003-X Section 6.2 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5 where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS. Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Regarding the concern that the draft language established a higher bar than similar requirements in CIP-005, clarifying changes have been made to the standard and technical rationale to address this concern. The use of the language	

was to ensure that industry understood that the Team was scoping this requirement to focus on low impact BES cyber systems. The SDT had several conversations about this topic including discussions with NERC compliance and legal staff. The team determined, based on these discussions and a reading of the Supply Chain report, that the SAR and the NERC Board resolution: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes that a considerable amount of research would be needed before many respondents would be able to provide a well-informed answer to this question. We note that the December 2019 “Supply Chain Risk Assessment” report states, “More than 99% of the responders (to a survey question about costs and benefits) agreed with the draft response that it was premature for CIP-013 registered entities to determine or estimate costs or benefits associated with the implementation of the standard…” That said, N&ST believes the cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands that there may be technology and procedural costs associated with the proposed draft standard.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

BHE expects Section 6.2 implementation to require additional technology and resources over and above Section 3 requirements. The concern is with the supply chain timelines and physical implementation across a great many assets containing low impact BES Cyber Assets. The large scope will take time to implement and may also require a significant monetary expenditure. While the SDT cannot do anything to mitigate costs, the implementation timeline can be expanded to allow for what will be a project of greater scope than any similar projects affecting only medium and high impact BES Cyber Assets.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the risk are defined in the Supply Chain report and asserts that the draft language in CIP-003-X meets the goals laid out in the SAR and the NERC Board resolution which was based on that report.	
Teresa Krabe - Lower Colorado River Authority - 5	

Answer	No
Document Name	
Comment	
If current procedural controls are not sufficient to achieve compliance, then there will be additional costs. Additional licensing that is expensive may be required. Where is there sufficient risk to warrant the increase in cost?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the risk are defined in the Supply Chain report and asserts that the draft language in CIP-003-X meets the goals laid out in the SAR and the NERC Board resolution which was based on that report.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The broad scope of the proposed language appears to bring all low impact assets into scope as it requires all communication to all assets be monitored at alkl times for malicious communication through vendor remote access, whether the access is being utilized or not.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The use of the language was to ensure that industry understood that the Team was scoping this requirement to focus on low impact BES cyber systems.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	No
Document Name	
Comment	
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost effectiveness of the approach to compliance cannot accurately be determined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to questions 1 and 2.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The MRO NSRF does not believe that the modifications are cost effective within the confines of the current implementation plan. The implementation of security measures for vendor remote access at the vast amount of assets containing LIBCS, often remotely located, would be highly impactful to entities' budgets and may require a phased-in approach to spread costs over several fiscal years.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
Until the technical issues referenced in response to questions 1 and 2 are addressed, the cost-effectiveness of the approach to compliance cannot accurately be determined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to questions 1 and 2.	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Sect. 6.2, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications," is impractical. When CTG OEMs interrogate our DCSs for long-term service agreement purposes we verify the identity of the requestor and throw a switch to grant them access, but as they collect data it is not possible to identify and deter in real time any risky communications. Verifying that the requestor is an authorized representative of the OEM should be sufficient.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT does not believe that allowing them to connect and verifying their identity is sufficient. The purpose of the SAR was to increase the security around the connection and the SDT believes that the words drafted in the standard meet the intent of the SAR. In addition, the SDT would like to point out that no time frames are specified in the draft language of proposed CIP-003-X.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends this project may be a good avenue to incorporate low impact requirements into these standards to avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has confined these changes to CIP-003-X so that entities without High or Medium impact assets are required to be in compliance with a smaller set of standards, as it is currently. Additionally, the SAR for Project 2020-03 was scoped to focus solely on CIP-003.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	

The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to. Cost to achieve compliance with Attachment 1, Section 6.2 at low impact locations, which goes above and beyond medium and high location requirements, may not be cost effective	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT defers to the NERC Rules of Procedure for registered entity compliance accountabilities. Regarding the concern that the draft language established a higher bar than medium and high location requirements, clarifying changes have been made to the standard and technical rationale to address this concern.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA does not believe that adding an additional requirement to Low systems over current M/H requirements is cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Regarding the concern that the draft language established a higher bar than medium and high location requirements, clarifying changes have been made to the standard and technical rationale to address this concern.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No

Document Name	
Comment	
The changes as written in Section 6.2 would require implementation of equipment/processes for monitoring communications at each Low Impact BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands that there may be technology and procedural costs associated with the proposed draft standard.	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Given the ambiguity around what constitutes “vendor remote access” it is difficult to determine what it would take to comply with the proposed requirements or determine if the modifications would be cost effective. Would a contractor that is issued an entity provided/managed laptop, working from an entity owned facility, that has been onboarded using the same process as all entity employees that have been granted unescorted and electronic access still be considered a vendor? The cost and implementation could be quite significant if entities were to have to renegotiate contracts and get access to assets for which they are registered for, but that they do not have access to.	
Likes 1	Platte River Power Authority, 5, Archie Tyson

Dislikes 0	
Response	
Thank you for your comment. The Team has revised the drafted standard and technical rationale to clarify the use of this term. The SDT defers to the NERC Rules of Procedure for registered entity compliance accountabilities.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
TMLP believes that the cost of implementing these additional protections will not be overly burdensome in the sense of adding equipment, but the time that it takes to complete small daily/regular tasks may be increased and therefore may increase labor expenses.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT understands that there may be technology and procedural costs associated with the proposed draft standard.	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF's comments for Question 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to MRO NSRF.	
Michael Jang - Seattle City Light - 1	

Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP agrees that the proposed modifications are cost-effective so long as a couple criteria are met: • The proposed language AEP has suggested in response to Question #1 is incorporated in Attached 1 Section 6. Proving the negative is burdensome to the Responsible Entity, and the proposed language will ensure Responsible Entites are not required to do so should they not have vendor remote access implemented as part of their business process. Please see AEP's response to Question #1 above. • The solution to meet the vendor remote access requirements can be implemented at the network or perimeter level rather than at the device or substationlevel.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to question 1. The SDT believes that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant

Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply.	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
This question is very utility specific; for some smaller utilities this may be more difficult and costly to implement than it would be for larger utilities. This brings into question if the risk that the smaller utilities presents is commensurate with the increased expenditure.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT understands the cost is variable between smaller and larger utilities and asserts that the proposed draft standard allows each entity to consider their unique security environment when creating their plan in order to comply.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel/vendors appropriately.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

We do not believe that the technology exists to identify and deter in real time any risky communications by the OEM when interrogating the DCS, nor is it likely to become available in the next eighteen months.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team believes that there are ways to meet the standard as drafted. Please review the technical rational and Attachment 2 for more information.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO supports the NPCC submitted comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to NPCC comments.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI recommends a 24-month impelemntation plan given the large vendor solution diversity within a very non-homogenous array of low-impact facilties. Entities may need to compile a inventory of applicable Cyber Assets to determine the impact of the proposed requirements as entities are currently not required to maintain a discrete listing of Cyber Assets at low impact facilities, which are most likely to contain multiple vendor solutions. This extended implementation plan provides entities sufficient time to conduct an inventory of applicable BCAs and BCSs, and implement additional electronic access controls which may be both procedural and technical in nature.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy generally supports EEI comments. A minimum 36 month implementation period, based on the current broad scope of the proposed standard impacting DERs, which are rarely manned but have remote access for operations, would be necessary to design, install, and train for new equipment and capabilities.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases, design and training to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	

An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
An entity that has high and medium impact BCS in addition to low impact facilities would have an easier time implementing these requirements; however, an entity that is only low impact would have a challenging time meeting this the 18-month implementation timeframe. At least a 24-month timeframe should be considered.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT asserts that the current draft standard does not require an inventory of low impact BES cyber assets.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the time, effort, and cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3. N&ST recommends a 24 month implementation time frame.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends a longer implementation plan e.g. ~ 36 months considering the cost and scope impact as identified in comments of Question 4 and 1 above. Once the clarity of terms and definitions as identified per our comments to Questions 1 and 4 is obtained, BC Hyrdo will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	

Comment	
The requirement to review and affect changes need a longer duration to implement. An implementation plan of a minimum of 36 months to complete the changes. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Recommend a 24-month implementation	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	

Answer	No
Document Name	
Comment	
We suggest 24 months because of the number of assets with low impact BCS.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Cynthia Lee - Exelon - 5	

Answer	No
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institute's (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment
SIGE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations will take much more time.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment
Recommend a 24-month implementation due to the significant scale of Low Impact. As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT has the task to improve operational security and believes that this standard increases security at Low impact sites.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	
MPC supports MRO NERC Standards Review Forum comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to MRO NERC Standards Review Forum comments.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
With most entities budgeting 18-24 months in advance, for new infrastructure and staffing resources, this could be a problematic timeline. The Entity would need to update their processes, procedures, train staff, hire resources, and implement technology. All this would need to be completed once budget has been approved. Based on Entity budgeting and the multiple items that will need to be address we would suggest 24-36 months.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF recommends that the proposed implementation plan be modified to allow for 24-36 months following the effective date. This timeframe will allow entities to implement the necessary hardware/software, procedural, and vendor contract changes at low impact facilities.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	

Comment	
See comment provided by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA suggests that 24 months be given for implementation to procure, configure, install, train and write procedures associated with the task of detecting malicious communication.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No

Document Name	
Comment	
Presently, there is no requirement obligating a "low" asset list. We believe that these changes would require compiling a detailed list. In our opinion because we have a vast amount of low Cyber Systems, 18 months would not be adequate time to compile and validate such a list.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT asserts that the current draft standard does not require an inventory of low impact BES cyber assets.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT asserts that the current draft standard does not require an inventory of low impact BES cyber assets.

Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	

Comment
AZPS feels that a 24-month implementation plan would be a reasonable timeframe to implement process, procedures or technology to meet the proposed language in Section 6. It may be necessary to design and implement multiple solutions to meet the proposed language in Section 6 across the various environments in which low impact assets are in use. Alternatively, a single solution which could be applied across a broader group of low assets may require significant design changes to process, procedures and/or technology.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases, design and training to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment	
CEHE does not agree the proposed timeframe provides enough time to put into place process, procedures, or technology to meet the proposed language in Section 6. Some entities have a higher number of low impact systems than medium or high impact systems, therefore deploying technology to these locations may take much more time. CEHE recommends a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No

Document Name	
Comment	
MISO supports comments submitted by the MRO NSRF. The implementation of security measures, such as IDS/IPS, for vendor remote access at a vast amount of assets containing LIBCS would be impactful to entities' budgets and may require a phased-in approach over 36 months to spread costs over different fiscal years. The phased-in approach could have an initial effective date begin at 18 months for Sections 6.1 and 6.3 and conclude with full implementation of 6.2 at 36 months.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to MRO NSRF.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Due to the number of assets potentially affected by the proposed changes and high likelihood that additional technical controls will need to be implemented, 18 months would not be adequate to implement the proposed measures. To allow for budgetary allocation and implementation for technical measures needed to comply with the proposed changes, GSOC recommends a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of	

Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
OKGE supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
18 months is not adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to implement substantial new protections for low impact BES Cyber Assets in order to monitor and control vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess & document vendor-specific remote access at all of their affected facilities, which is a significant undertaking. Given the current supply chain issues/delays underscores the substantial and impacts on entities' ability to timely secure materials necessary to implement these changes. For these reasons, the implementation plan should be a minimum of 36 months. In addition, Attachment 1, Section 6, part 6.2 could be understood to require entities to install IDS-like solutions for low impact BCS. Given the large number of locations and the efforts that will be required to implement 6.2 and the aforementioned supply chain	

delays, 36 months is more than reasonable . While a phased approach may be another solution, the logistics of effectively implementing a phased approach will be difficult to both budget, administer and audit.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. Please see the technical rationale for a discussion on IDS/IPS.	
Gail Golden - Entergy - Entergy Services, Inc. - 1,5	
Answer	No
Document Name	
Comment	
Additional time of 24 months due to potential funding cycles needed for implementation	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No

Document Name	
Comment	
BHE does not agree that 18 months is adequate to implement these changes. The impact of the proposed changes will be significant and require many affected registered entities to compile detailed lists of low impact BES Cyber Assets and vendor remote access permissions associated with those assets. It is also important to recognize that affected companies will be required to identify, log, assess and document remote access at all of their affected facilities, which is not an inconsequential task. For these reasons, the implementation plan should be on the order of 24 to 36 months.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT asserts that the current draft standard does not require an inventory of low impact BES cyber assets.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Recommend a 24-month implementation due to the significant scale of Low Impact. As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see. The SDT has the task to improve operational security and believes that this standard increases security at Low impact sites.	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
If the scope is clear, 18-months for implementation should be fine. Given some of the ambiguity in the current draft, more specifically, the lack of clarity of key terms, it is difficult to determine the extent of changes or what additional technical resources necessary to comply. Additionally, some entities may have very limited security technologies in place for or at low impact assets that can be re-used for the purpose of meeting the requirements. For those entities, it may take much more time to architect, procure, and deploy a solution. Given the potentially large number of low impact sites, 18-months could be challenging.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The SDT has made clarifying changes to Section 6 and thus the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more	

logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Brian Belger - Seattle City Light - 6	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP believes the 18-month implementation plan allows for enough time so long as:	

- the requirement is applicable to Responsible Enties that have implemented vendor remote access as noted in the response to Question #1, and
- the solution to meet the vendor remote access requirements can be implemented at the network-level rather than at the device-level as noted in our response to Question #4. Should that not be the case, a 36-month implementation plan would be more appropriate.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT has made clarifying changes to Section 6 and thus the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.

Michael Jang - Seattle City Light - 1

Answer	Yes
Document Name	

Comment

Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of

Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports the MRO NSRF's comments for Question 5.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Please see response under MRO NSRF.	
Hao Li - Seattle City Light - 4	
Answer	Yes
Document Name	
Comment	
Instead of an 18-month plan, an implementation plan could be broken down to a few phases, which each phase has its milestones. This approach will allow small entities with no resources to find ways to implement gradually while large entities with more resources may implement all in once.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes the 18-mont implementation plan can be achieved base on our current setup but understands the concerns raised in the EEI comments related to supply chain delays for other entities and would be willing to support a 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	

Our specific system will not have a problem trying to meet an 18-month implementation plan, but we do have some concerns for the entire Low Impact category due to the large amount of entities who fall under this category, and the varying degree of size and abilities of the entities who fall under this category. Some entities may be less equipped to handle these issues than others.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Pend Oreille County, 5, Kramer Bryant
Dislikes 0	
Response	
Bryant Kramer - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
April Owen - Public Utility District No. 1 of Pend Oreille County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Curtis - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	
Document Name	
Comment	
Unable to comment on this.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Donna Wood - Tri-State G and T Association, Inc. - 1	

Answer	
Document Name	
Comment	
Tri-State does not agree with an 18-month implementation plan. Again, applying section 6 to facilities containing low impact BES may require significant costs in hardware (Firewall upgrades) or additional out of band circuits, etc.) to be able to detect and disable VRA at remote and/or unmanned locations. A longer phased-in approach would be more appropriate for planning and budgeting purposes. Tri-State suggests a 36 month phased-in approach.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment and the implementation timeframe has been adjusted. After much debate among the team, NERC staff and FERC staff, the SDT felt a staggered approach would be more logical. The SDT settled on 18 months for implementation of Sections 6.1 and 6.2 and then Section 6.3 is 6 months after 6.1 and 6.2 (for a total implementation time of 24 months for Section 6.3). This allows any equipment purchases to span a full budget cycle and the SDT is hoping it address any supply chain issues entities may see.	

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.
Russell Noble - Cowlitz County PUD - 3

Answer	
Document Name	

Comment
I also support comments provided by Utility Services.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1

Answer	
Document Name	

Comment
TMLP believes that it may be necessary to require the vendor provide the Registered Entity with logging information about who and what was done during the remote session. While we recognize that this was listed as one of the options in the CIP-003-X Attachment 2 for Section 6, we believe that this should be required in some manner.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment and believes in a risk based model supported by both NERC and FERC, the entities should be free to create a process and/or plan that meets their internal process the best, thus we are not being specific in how entities meet the required objectives.
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5
Answer
Document Name
Comment
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access. a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA. b. VRA needs to be limited to access to BCS. c. VRA must allow the use of CIP-003-8, reference model 3. 2) There are a number of issues with the CIP-003-X Technical Rationale a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access. b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents. c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.

a. The technical rational (TR) for 6.2 states: "The obligation in Section 6.2 requires that entities which allow vendor remote access." We request updating the Requirement by adding "vendor remote access." To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase "active vendor remote access sessions". 6.1 and 6.3 do not include the word "active". Without the word 'active', 6.1 and 6.3 could include or maybe be limited to "capability" of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses "that are taking place" and the TR for 6.3 uses "active". Sections 6.1, 6.3 and the TR should consistently use the word "active".

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA's. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	
Document Name	
Comment	

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. ATC requests the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements. Additionally, please consider abandoning the use of the undefined term "vendor remote access" and finding language that explicitly removes the read only sharing of information falling under the umbrella of 'remote access'. ATC requests consideration of alternative language such as: Requirement "***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***". Carry this concept through to Attachment 1 Section 6.

Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment. The Team decided that keeping "Declaring and responding to CIP Exceptional Circumstances" at the bottom of the list was the best route. By adding things below it could be perceived that a CIP Exceptional Circumstance only applied to those instances above and not those below.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	
Comment	

As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures.

BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC prefers to retain the Technical Rationale, especially verbiage that limits scope to Low Impact and Interactive Remote Access. Furthermore, ITC believes this requirement is not as cost effective as mentioned by EEI. In Section 6.2 a requirement to scan traffic for suspicious, malicious communication requires specialized equipment and/or processes. Today, this is only necessary under CIP-005-6 R1.5 for High Impact. The impression is that we're talking about skipping Medium and going to Low. This does not appear to follow a risk based approach.	
Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI also notes that the SDT did not request comment on the modifications to Requirement 1, subpart 1.2 which is material to the draft. In the modifications to this section, we note that the SDT has used the undefined term "vendor remote access", while leveraging this key term in both Requirement 1, subpart 1.2.6 and Attachment 1, Section 6 even though this term is not well understood by the industry. EEI recommends defining of this term. (See our comments to Question 1)

Additionally, EEI believes it may be more efficient and effective over time to simply reference all parts of Attachment 1 within Requirement 1, subpart 1.2 rather than modifying Requirement 1 each time changes are made to the requirements associated with CIP-002, containing low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	

We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions:

While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS.

Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E has no additional comments on the modifications.

Likes 0	
Dislikes 0	

Response	
Sarosh Muncherji - British Columbia Utilities Commission - 9	
Answer	
Document Name	
Comment	
There is the usual direct supply chain where specific vendor products are utilized for BES cyber system operations and maintenance. There are other sources of software that may possibly be overlooked as being part of the "supply chain" and these products may slip through the cracks. Examples include freeware utilities such as text editors (for example, NotePad++) and communications programs (for example, PuTTY). The SDT may consider requiring software integraty validation for all software in a future revision to the standard.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. Those requirements are outside our current SAR. We will pass this comment along.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
Of significant note, the proposed changes do not reference protecting only a routable communication medium, leaving the language unclear as it relates to non-routable connections as might be found in low-impact field equipment. Similar requirements in medium-impact systems are only required at Control Centers as reflected in CIP-005 R1.5 or are otherwise qualified based on the connectivity of the cyber asset, e.g., CIP-005-6, R2.4, R2.5. Thus, the proposed requirements for low-impact assets require greater protections across	

a larger swath of assets than the ones governing medium-impact assets. The proposed language, therefore, raises the protections of low-impact assets to that of high-impact assets, thereby removing any risk-based differentiation of controls between impact ratings.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. We have made modifications to the standard and believe by clarifying the connections to be those managed by CIP-003 Section 3 Electronic Access Controls, we have addresses this concern.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	
Document Name	
Comment	
Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman	
Answer	
Document Name	

Comment
Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	
Document Name	

Comment
As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures. BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows. BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
We request that the Guidelines and Technical Basis are not removed from the standard. The Technical Rationale document released with these changes only addresses the new Section 6 changes, and does not replace the comprehensive Guidelines and Technical Basis currently in the standard. The current Guidelines and Technical Basis are used as reference documentation by NERC Regional Entities and Generator Owners, and we believe have played a critical role in the development of compliance programs and internal controls.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, however, NERC has determined that the Guidelines and Technical Basis had to be removed from all standards going forward.	
Hao Li - Seattle City Light - 4	
Answer	
Document Name	
Comment	

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements. Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X.

Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment. The Team decided that keeping “Declaring and responding to CIP Exceptional Circumstances” at the bottom of the list was the best route. By adding things below it could be perceived that a CIP Exceptional Circumstance only applied to those instances above and not those below.

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	

Comment
Comments: Section 6, items 1-3 appear to try and address the 3 separate Board Resolution recommendations as vendor remote access. Each should be addressed separately to ensure revision clarity. As stated above in the answers to questions 1&2 the language is not specific. Is this for detection methods for all inbound and/or outbound communications? For example, if you use a data diode, would you still need to detail a method for monitoring all inbound and outbound malicious communications?

Likes 0	
Dislikes 0	

Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
See comment provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF supports preserving the language identified for deletion in Section 6 – Background and Attachment 2 – Guidelines and Technical Basis (GTB).	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, however, NERC has determined that the Guidelines and Technical Basis had to be removed from all standards going forward.	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	
Document Name	
Comment	
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
When the CIP-005 R2.4-2.5 requirements were added, entities were able to leverage existing monitoring systems and infrastructure in their High and Medium Impact Control and Data Center environments (IDS, IPS, SEIM, Intermediate Systems, etc…). Additionally, with remote Medium Impact sites, entities were already required to institute use of an Intermediate System for IRA. For assets containing Low Impact BES Cyber Systems, typically unmanned and with fewer applicable requirements, this type of infrastructure is often not in place. With the high volume of Low Impact sites, this could pose an enormous and untenable burden on RE's.	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	
Document Name	
Comment	
MPC has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access. a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA. b. VRA needs to be limited to access to BCS.	

c. VRA must allow the use of CIP-003-8, reference model 3. 2) There are a number of issues with the CIP-003-X Technical Rationale a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access. b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents. c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
SIGE would like additional clarity within the technical rationale as to whether virtual meeting sessions (e.g. such WebEx or Zoom meetings where the screen is shared, either escorted or unescorted) are considered vendor remote sessions. **Additionally, "asset" needs to be defined within the NERC Glossary of Term. "Asset" can be interpreted in many ways which may lead to inconsistent application of the requirements or definitions it is used in.**	
Likes 0	
Dislikes 0	

Response	
Aric Root - CMS Energy - Consumers Energy Company - 4	
Answer	
Document Name	
Comment	
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to EEI's comment.	

Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to EEI's comment.	
George Brown - Acciona Energy North America - 5	
Answer	
Document Name	
Comment	
Acciona Energy has no additional comments at this time, thank you for your consideration.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	

Comment
1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access. a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA. b. VRA needs to be limited to access to BCS. c. VRA must allow the use of CIP-003-8, reference model 3. 2) There are a number of issues with the CIP-003-X Technical Rationale a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access. b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents. c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models. 3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist. a. The technical rational (TR) for 6.2 states: "The obligation in Section 6.2 requires that entities which allow vendor remote access." We request updating the Requirement by adding "vendor remote access." To be consistent with 6.1 and 6.3. 4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase "active vendor remote access sessions". 6.1 and 6.3 do not include the word "active". Without the word 'active', 6.1 and 6.3 could include or maybe be limited to "capability" of the vendor or the BES configuration and electronic access controls.

a. The TR for 6.1 uses “that are taking place” and the TR for 6.3 uses “active”. Sections 6.1, 6.3 and the TR should consistently use the word “active”.

b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA’s. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has chosen to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment, please see the response to EEI's comment.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has chosen to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see the response to EEI's comment.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
Vendor remote access (VRA) is not a defined term Request clarification on "malicious communications" In case there is no "vendor remote access", which evidence is to be produced ?	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy has a higher volume of low impact locations as compared to high or mediums. A significant amount of prerequisite work must be done in order to come into compliance with the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	
Recommend the SDT address the term "system-to-system" by looking at CIP-002. This would greatly help industry by removing a meaningless phrase and helping industry by providing them a way to parse systems owned and used by vendors, systems owned by entity's but used by vendors, and/or systems owned and used by entities for remote access. Recommend the SDT look at CIP-004 R4 to authorize vendors because it would align the concept of authorized vendors within the existing authorization standards and then only the systems used for access would need to be addressed in CIP-002 (recommendation 1)	
Likes 0	
Dislikes 0	
Response	

Michael Jang - Seattle City Light - 1	
Answer	
Document Name	
Comment	
The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements. Additionally, please consider abandoning the use of the undefined term "vendor remote access" and finding language that explicitly removes the read only sharing of information falling under the umbrella of 'remote access'. We request consideration of alternative language such as: Requirement "***R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS***". Carry this concept through to Attachment 1 Section 6 to remove "vendor remote access" from use in CIP-003-X.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment. The Team decided that Declaring and responding to CIP Exceptional Circumstances" at the bottom of the list was the best route. By adding things below it could be perceived that a CIP Exceptional Circumstance only applied to those instances above and not those below.	
JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	
No additional comments. AEP would like to express thanks to the standard drafting team's hard work on this project.	

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
Tacoma Power recommends clarifying that Attachment 2, Section 6 applies to vendor's access to low impact assets containing BES cyber systems from remote locations, as follows:	

• Attachment 2, Section 6, Bullet 2: "2. Documentation of configuration of security alerts; security alerts or logging relative to activities during the **vendor remote** communication from items such as:" • Attachment 2, Section 6: "**Vendor Remote Access:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:"	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	
Document Name	
Comment	
BC Hydro ackowledges the effort and hard work by SDT which went into putting together these complex changes to CIP-003-X. As identified in comments to Question 1 and 4 above, the definitions of terms and clarity of application with some specific industry use case examples will provide a clear understanding and will help to get a faster and appropriate approvals of these proposed changes.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	

N&ST has reviewed the January 2020 NERC Member Representatives Committee "Policy Input Package" that preceded the February NERC Board meeting, and it is our principal observation that there was not a strong consensus among the members about the best approach to address concerns about coordinated attacks on low impact assets with vendor remote electronic access as the primary attack vector. We also noted that there were several suggestions to the effect that more comprehensive cost-benefit analyses should be performed before extending the scope of Supply Chain requirements to include low impact assets containing BES Cyber Systems.

N&ST notes the proposed requirement to require malicious communications detection at low impact assets containing BES Cyber Systems would, if effected, result in a more stringent requirement being imposed on low impact assets than on medium impact BES Cyber Systems with External Routable Connectivity at facilities other than Control Centers. N&ST is aware that the December 2091 NERC "Supply Chain Risk Assessment" raised the specter of coordinated, common mode attacks on large numbers of low impact assets, stating, "This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System." While we acknowledge this possibility and agree it is of some concern, it is our opinion that it may make more sense, and achieve a better return on investment, to add a malicious communications detection requirement for medium impact first.

It is N&ST's opinion that introducing the concept of lower-case "interactive" vendor remote access to BES Cyber Systems at low impact assets will cause needless confusion among entities subject to requirements for upper-case Interactive Remote Access, and therefore we recommend that it be dropped. We see no need to distinguish "interactive" vendor remote access from "system-to-system" vendor remote access in CIP-003.

Likes 0	
Dislikes 0	
Response	
Brian Belger - Seattle City Light - 6	
Answer	
Document Name	
Comment	

The SDT did not ask industry for perspectives on modifications to the parent Requirement R1.2; which is material to this draft. We request the SDT please consider moving the newly proposed requirement R1.2.6 to the end of the list as R1.2.7 so Registered Entities do not have undue administrative burden to renumber within existing documentation because of shifting of other requirements.

Additionally, please consider abandoning the use of the undefined term “vendor remote access” and finding language that explicitly removes the read only sharing of information falling under the umbrella of ‘remote access’. We request consideration of alternative language such as: Requirement “**R1.2.7. Electronic access that permits a vendor to perform remote command and control functions of the low impact BCS**”. Carry this concept through to Attachment 1 Section 6 to remove “vendor remote access” from use in CIP-003-X

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment. The Team decided that keeping “Declaring and responding to CIP Exceptional Circumstances” at the bottom of the list was the best route. By adding things below it could be perceived that a CIP Exceptional Circumstance only applied to those instances above and not those below.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

This includes systems used by vendors for system-to-system remote access and vendor "Interactive Remote Access (IRA)" (delete words in quotes) interactive remote access to low impact BES Cyber Systems.

Reasoning: The NERC defined term Interactive Remote Access includes the Electronic Security Perimeter, which is not a concept in CIP-003-8. Suggest using lowercase interactive remote access as is used in Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access section of the document.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	
Document Name	
Comment	

As mentioned in Q1, BHE wishes the technical rationale document to address the intended scope of vendor remote access with respect to vendor read-only access. BHE would not expect vendor read-only access, which could be used for health monitoring, to be a risk requiring Section 6 protective measures.

BHE proposes the the last sentence of Rationale Section 6 of Attachment 1, “This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems” be revised to ”This includes systems used by vendors for interactive and system-to-system remote access to low impact BES Cyber Systems, excluding read-only access.” Please note that Interactive Remote Access cannot be used in conjunction with low impact BES Cyber Assets as this term is dependent on ESPs or EAPs which are not applicable terms for lows.

BHE also requests the following guidance be added to the technical rationale document: vendor remote access is access from vendor owned or managed assets to a CIP applicable system. A vendor or contractor using a Registered Entity owned Cyber Asset to access CIP applicable systems via Registered Entity’s network is not considered vendor remote access.

Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 3, Gresham Darnez
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	

Answer	
Document Name	
Comment	
Nothing additional at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE has the following additional recommendations for the SDT:

- Include language for (1) software integrity and authenticity, (2) info system planning and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010.
- Include vendor multi-factor authentication (MFA). Passwords can be subjected to numerous cyber-attacks, including brute force. MFA provides an additional layer of security and protects systems should passwords become known by unauthorized users.
- Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.

Texas RE also notes that the language proposed in Attachment 1, Section 6 utilizes the undefined term “interactive” in context to vendor remote access rather than the NERC defined term Interactive Remote Access (IRA). Since the current IRA definition is associated with ESPs, Texas RE would strongly encourage revising the IRA definition to include “assets that contain low impact BES Cyber Systems.” The definition of IRA would read: “User-initiated access by a person employing a remote access client or other remote access technology

using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's ***assets that contain low impact BES Cyber Systems***, Electronic Security Perimeter(s), or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications."	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 3	
Answer	
Document Name	
Comment	
PNMR believes there are substatial improvements to be made to provide clarity and consistency, not only within CIP-003 but also with CIP-005	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	

Attachement 2 Section 6 containes many capitalized terms that are not contained in the NERC glossary of terms. The SDT should consider not capitalizing the following terms: Security Information Management, Firewall, Intrusion Detection System, Intrusion Prevention System, Virtual Private Network, Remote Desktop, Removing, and Ethernet. By doing such the draft CIP-003-X Standard will further align with the usage of similar terms within the existing FERC approved CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	
Document Name	
Comment	
Please reference responses to questions 1 and 2.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The MRO NSRF has no additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Our main concern was for our market participants. The proposed addition of 6.2 for "malicious communications detection" is infrastructure dependant and could prove difficult for low impact facilities without the necessary supporting infrastructure. While we accept the reasoning for it's proposed inclusion, we would prefer "6.2 Having one or more method(s) for detecting known or suspected malicious *communications for both inbound and outbound communications, per communications capability "* *Due to the large size and scope of any implementation, in particular for the proposed 6.2 requirement of "detect malicious communications", we would prefer to see a 24 month implementation period in order to allow enough time for entities to have a full budgeting and implementation cycle.*	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	

Answer	
Document Name	
Comment	
Please reference responses to questions 1 and 2.	
Likes 0	
Dislikes 0	
Response	
Kevin Lyons - Central Iowa Power Cooperative - 1	
Answer	
Document Name	
Comment	
While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. The revisions being made to CIP-003-X create more stringent controls for low impact BCS than are currently required for medium impact BCS. While this new requirement was part of the NERC study, low impact BCS should not have to meet greater requirements than higher impact level BCS. Our position is that the same revisions should be made for medium impact BCS, whether through additional work in this project or through another project. Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends once virtualization/zero trust architecture is implemented the SDT start focusing on incorporating low impact requirements into the other standards where applicable and change the applicable systems of the other standards to include low impact BCS. Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
This Standard brings in some medium/high impact requirements for low impact. The proposed language brings in a subset of the CIP-005 requirements, which creates more stringent controls for low impact BCS than medium impact.	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	
Document Name	
Comment	
We believe that requirements for controlling remote access are adequately addressed by Section 3: Electronic Access Controls, and therefore find the proposed Section 6 unnecessary.	
Likes 1	DTE Energy, 4, ireland patricia
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	
Document Name	
Comment	
NA.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	
Document Name	
Comment	
Definitions for Vendor remote access and what constitutes malicious communications would provide some clarity and help entities determine the cost effectiveness standard. SMUD suggests changing lower case “asset” to “facility” to remove the confusion that already exists. Moving requirement 6.2 to section 3 might make it more consistent with CIP-005.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
AEPCO has signed on to the ACES comments below: We would like to thank the SDT for preparing the changes and allowing us to comment. We do have a concern not addressed by the above questions:	

While the revisions address the risk of malicious communications outlined by the NERC Board resolution, this is NOT a requirement for medium impact BES Cyber Systems not at Control Centers. This was brought up by ACES at the final CIPC meeting as CIP-005 R1.5's applicable systems are high impact and medium impact BES Cyber Systems at Control Centers. This creates more stringent controls for low impact BCS, than medium impact BCS which we object to. While this new requirement was part of the NERC study low impact BCS should not have to meet greater requirements than higher impact level BCS. Further, there is not an existing project to change CIP-005 R1.5 to include all medium impact BCS and the CIP-005 revision from Project 2016-02 do not change the Applicable Systems to include medium impact BCS not at Control Centers. Without adding medium impact BCS to CIP-005 or removal of this proposed requirement, the standards will leave a gap for medium impact BCS not at a Control Center when considering malicious communications.

Likes 0	
Dislikes 0	
Response	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Initial Ballot and Non-binding Poll Open through October 11, 2021

Now Available

The initial ballot for **CIP-003-X - Cyber Security — Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, October 11, 2021**.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.
For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Open through October 11, 2021
Ballot Pools Forming through September 27, 2021

Now Available

A 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls**, is open through **8 p.m. Eastern, Monday, October 11, 2021**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team will post CIP-003 with a –X version letter at the end and Virtualization will post CIP-003 with a –Y. The version number will be assigned upon adoption by the NERC Board of Trustees.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, September 27, 2021.** Registered Ballot Body members can join the ballot pools here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted October 1-11, 2021.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/234)
Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X IN 1 ST
Voting Start Date: 10/1/2021 12:01:00 AM
Voting End Date: 10/11/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 243
Total Ballot Pool: 292
Quorum: 83.22
Quorum Established Date: 10/11/2021 3:52:51 PM
Weighted Segment Value: 29.2

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	78	1	16	0.258	46	0.742	0	3	13
Segment: 2	6	0.2	0	0	2	0.2	0	2	2
Segment: 3	69	1	14	0.237	45	0.763	0	3	7
Segment: 4	20	1	5	0.294	12	0.706	0	1	2
Segment: 5	64	1	15	0.294	36	0.706	0	1	12

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	48	1	13	0.351	24	0.649	0	0	11
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	5	0.3	1	0.1	2	0.2	0	1	1
Totals:	292	5.6	65	1.635	167	3.965	0	11	49

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Mike Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Steve Ritscher		Negative	Third-Party Comments
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Third-Party Comments
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Kevin Frick		None	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Great River Energy	Gordon Pietsch		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		None	N/A
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	Seattle City Light	Michael Jang		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Taunton Municipal Lighting Plant	Devon Tremont		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Wind Energy Transmission Texas, LLC	Bradley Collard		Abstain	N/A
2	California ISO	Darcy O'Connell		None	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Third-Party Comments
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Evergy	Marcus Moor		None	N/A
3	Eversource Energy	Christopher McKinnon		Abstain	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		None	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		Negative	Third-Party Comments
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	Manitoba Hydro	Mike Smith		None	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	Portland General Electric Co.	Adam Menendez		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	American Public Power Association	Jack Cashin		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Negative	Comments Submitted
4	DTE Energy	patricia ireland		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	George Brown		Negative	Comments Submitted
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Colleen Peterson		Negative	Third-Party Comments
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Third-Party Comments
5	Evergy	Jeremy Harris		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young	Helen Zhao	None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		None	N/A
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer		None	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 1 of Pend Oreille County	April Owen		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
7	Amazon Web Services	Kristine Martz		None	N/A
9	British Columbia Utilities Commission	Sarosh Muncherji		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 292 of 292 entries

BALLOT RESULTS

Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X | Non-binding Poll IN 1 NB
Voting Start Date: 10/1/2021 12:01:00 AM
Voting End Date: 10/11/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 232
Total Ballot Pool: 278
Quorum: 83.45
Quorum Established Date: 10/11/2021 3:34:44 PM
Weighted Segment Value: 28.65

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	74	1	13	0.245	40	0.755	9	12
Segment: 2	6	0.2	0	0	2	0.2	2	2
Segment: 3	68	1	11	0.224	38	0.776	12	7
Segment: 4	19	1	6	0.4	9	0.6	2	2
Segment: 5	60	1	13	0.31	29	0.69	6	12
Segment: 6	45	1	10	0.345	19	0.655	6	10
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	5	0.1	1	0.1	0	0	3	1
Totals:	278	5.4	55	1.724	137	3.676	40	46

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Mike Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Steve Ritscher		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		None	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Kevin Frick		None	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		None	N/A
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Taunton Municipal Lighting Plant	Devon Tremont		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Wind Energy Transmission Texas, LLC	Bradley Collard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		None	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Abstain	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		None	N/A
3	Eversource Energy	Christopher McKinnon		Abstain	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		None	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	Portland General Electric Co.	Adam Menendez		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	American Public Power Association	Jack Cashin		Affirmative	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Negative	Comments Submitted
4	DTE Energy	patricia ireland		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Comments Submitted
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Colleen Peterson		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Evergy	Jeremy Harris		None	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		None	N/A
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer		None	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Comments Submitted
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
9	British Columbia Utilities Commission	Sarosh Muncherji		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/18/20
SAR posted for comment	04/08/20
45-day formal comment period with ballot	August 27 – October 11, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	February 2022
10-day final ballot	April 2022
Board adoption	August 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Electronic vendor remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR	security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least	Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to	The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented electronic vendor remote access security controls but failed to document its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for	according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media	Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic vendor remote access security controls, but failed to implement electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Lower	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
X	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include:

6.1 One or more method(s) for determining electronic vendor remote access where such access has been established under Section 3;

6.2 One or more method(s) for disabling electronic vendor remote access where such access has been established under Section 3; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Electronic Vendor Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - Security Information Management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of:
   - Firewall policies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Virtual Private Network (VPN) hosts;
   - manual log reviews; or
   - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~second 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	03/18/20
SAR posted for comment	04/08/20
45-day formal comment period with ballot	August 27 – October 11, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 2021~~
45-day formal comment period with ballot	~~January~~February 2022
10-day final ballot	~~March~~April 2022
Board adoption	August 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None
~~None~~

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. ~~Vendor~~Electronic vendor remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high--level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR	security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least	Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to	The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented electronic vendor remote access security controls but failed to document its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for	according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media	Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic vendor remote access security controls, but failed to implement electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Lower	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
X	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6~~:~~ . Electronic Vendor ~~remote access~~Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access ~~(including interactive and system-to-system access) to low impact BES Cyber Systems that includes~~. These processes shall include:

6.1 ~~Having one~~One or more method(s) for determining electronic vendor remote access ~~sessions;~~where such access has been established under Section 3;

6.2 ~~Having one~~One or more method(s) for disabling electronic vendor remote access where such access has been established under Section 3; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications~~; and~~

~~**6.3** Having one or more method(s) for disabling vendor remote access~~.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

~~3.~~ Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~4.~~3.

Section 6. ~~**Section 6**~~ Electronic Vendor Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. ~~Documentation~~For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - Security Information Management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.

~~2. Documentation of configuration of security alerts; security alerts or logging relative to activities during the communication from items such as:~~

~~• For Section 6.2, documentation showing:~~ ~~Firewall policies;~~

~~• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~

~~• Virtual Private Network (VPN) hosts;~~

~~• manual review of logs; or~~

~~• other operational, procedural or technical controls.~~

~~6.~~2. ~~Documentation showing methods to disable vendor remote access such as:~~

- disabling vendor remote access user or system accounts;
- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of:

- Firewall policies;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;

- manual log reviews; or
- other operational, procedural, or technical controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-X — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Reliability Standard CIP-003-X

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-X, Requirement R2, Attachment 1, Section 6.3

Responsible Entities shall not be required to comply with Requirement R2, Attachment 1, Section 6.3 until six months after the effective date of Reliability Standard CIP-003-X.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-X as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-X.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-X within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-X — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Reliability Standard CIP-003-X

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-X, Requirement R2, Attachment 1, Section 6.3

Responsible Entities shall not be required to comply with Requirement R2, Attachment 1, Section 6.3 until six months after the effective date of Reliability Standard CIP-003-X.

Initial Performance of Periodic Requirements

~~Responsible Entities shall~~ Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially ~~comply~~ with ~~the~~those periodic requirements in ~~the Revised CIP Standards and Definitions~~CIP-003-X as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-X.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-X within the periodic timeframes of their last performance under ~~the Requested CIP Retired Standards and Definitions.~~ CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2020-03 Supply Chain Low Impact Revisions** by **8 p.m. Eastern, Monday, April 11, 2022.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Questions

1. Do you agree the updated language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-X

February 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

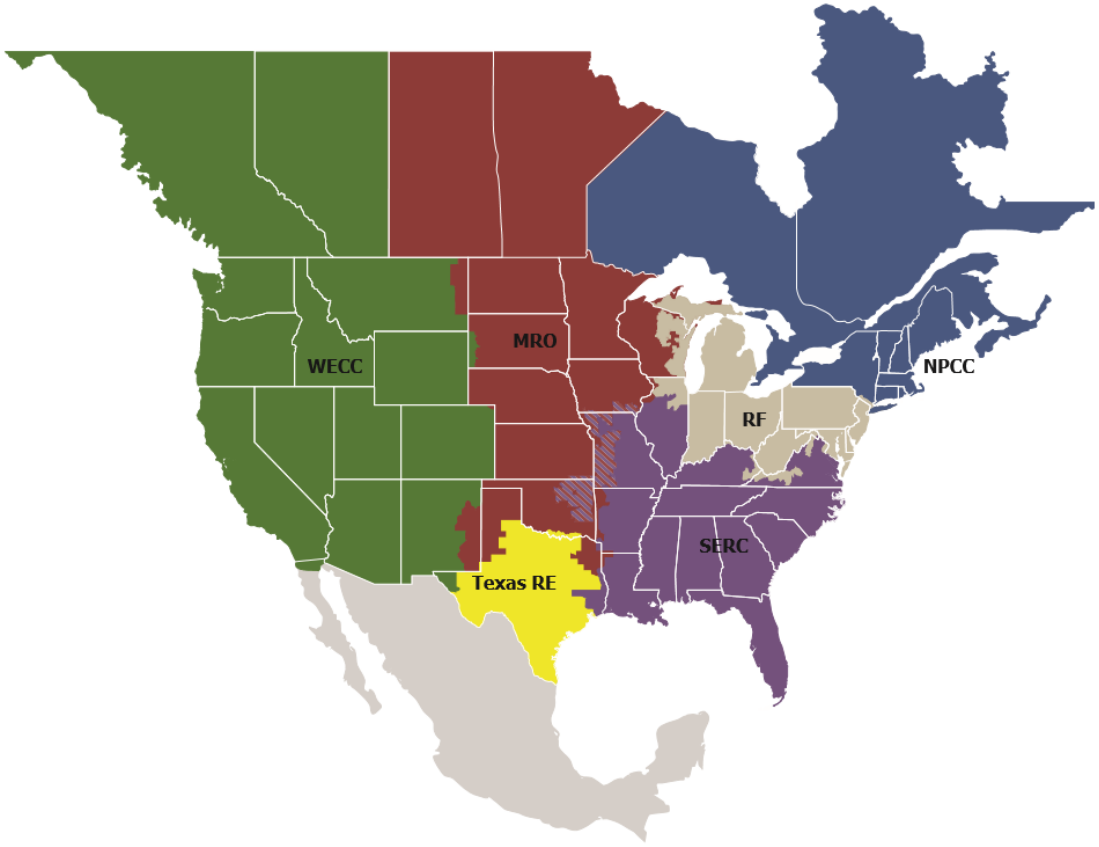
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language, the SDT reviewed and proposed multiple language options to clarify the requirements of electronic remote vendor access in context of existing Section 3 electronic access controls. In addition, the SDT considered process considerations, remote and electronic access, remote access architectures and technologies, and data paths communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining and disabling or terminating vendor electronic access.

The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use disparate processes, systems or technologies to manage vendor electronic access. The SDT also discussed systems and cyber assets owned by vendors but authorized for use on entity networks vs systems and cyber assets owned by entities but used by vendors for electronic remote access.

Given these multiple considerations the SDT established Section 6 to specifically address electronic vendor remote access and inbound/outbound malicious communications for low impact. The language requires an entity to develop and implement a process or processes for identifying electronic vendor remote access, having a method or methods for disabling electronic vendor remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

The language gives entities the flexibility to define processes to identify and manage electronic vendor remote access for their specific policies, processes, systems, configurations, organizations, operations, and Facilities. The language allows entities to define how and where electronic vendor remote access occurs and the ideal methods and timeframes to authorize, establish and disable electronic vendor remote access. Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling electronic vendor remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of external connectivity. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[1], and the resulting NERC Board resolution[2], the proposed Attachment 1 Section 6, as it relates to the existing Requirement 2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and electronic vendor remote access.

Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access

The objective of Attachment 1 Section 6.1 is for entities to have visibility of electronic vendor remote access on their low impact BES Cyber Systems. Such visibility increases an entity's ability to detect, respond and resolve issues that may originate with or be tied to a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have a method to determine electronic vendor remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable electronic vendor remote access in the event of a security event, the inability of a responsible entity to terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable electronic vendor remote access.

[1] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[2] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications by vendors, such that the entity may respond to and remediate resulting impacts. This sub part is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with low impact BES Cyber Systems.

Current Requirements in CIP-003-8 R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact BES Cyber Systems and medium impact BES Cyber Systems. Security controls such as use of intermediate systems and multi-factor authentication provide high impact BES Cyber Systems and medium impact BES Cyber Systems additional security from malicious communication and overall access controls. In addition to Intermediate Systems and multi-factor authentication, high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a Low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security Requirements to detect malicious communications under CIP-003-X Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-X

~~August 2021~~February 2022

~~RELIABILITY | RESILIENCE | SECURITY~~




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

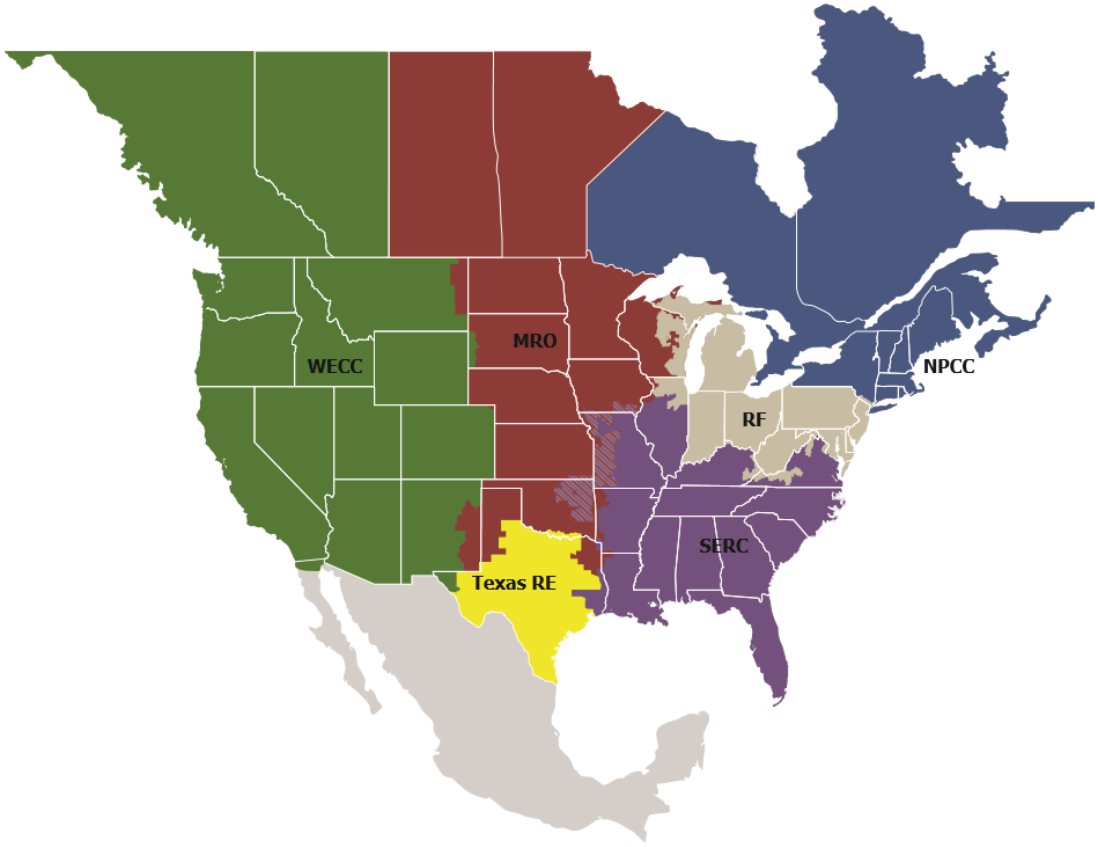
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language, the SDT reviewed and proposed multiple language options to clarify the requirements of electronic remote vendor access in context of existing Section 3 electronic access controls. In addition, the SDT considered process considerations, remote and electronic access, remote access architectures and technologies, and data paths communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining and disabling or terminating vendor electronic access.

The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use disparate processes, systems or technologies to manage vendor electronic access. The SDT also discussed systems and cyber assets owned by vendors but authorized for use on entity networks vs systems and cyber assets owned by entities but used by vendors for electronic remote access.

Given these multiple considerations the SDT established Section 6 to specifically address electronic vendor remote access and inbound/outbound malicious communications for low impact. The language requires an entity to develop and implement a process or processes for identifying electronic vendor remote access, having a method or methods

for disabling electronic vendor remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.
The language gives entities the flexibility to define processes to identify and manage electronic vendor remote access for their specific policies, processes, systems, configurations, organizations, operations, and Facilities. The language allows entities to define how and where electronic vendor remote access occurs and the ideal methods and timeframes to authorize, establish and disable electronic vendor remote access. Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling electronic vendor remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately ~~67~~66% have external connectivity which often results in the allowance of ~~3rd party access.~~external connectivity. As our grid has grown more complex, the use of ~~third~~external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected~~;~~. However, the prevalence of external connectivity ~~and 3rd party access, herein referred to as vendor[1] remote access,~~ across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[2], and the resulting NERC Board resolution[3], the proposed Attachment 1 Section 6, as it relates to the existing Requirement 2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and ~~vendor remote access. This includes systems used by vendors for system-to-system remote access and vendor Interactive Remote Access (IRA) to low impact BES Cyber Systems.~~electronic vendor remote access.

Attachment 1 Section 6 Part 6.1 – Determining Vendor Remote Access

The objective of Attachment 1 Section 6.1 is for entities to have visibility of electronic vendor remote access ~~sessions (including interactive remote access and system-to-system) that are taking place~~ on their low impact BES Cyber Systems. Such visibility increases an ~~entities~~entity's ability to ~~rapidly~~ detect, respond and resolve issues that may originate with or be tied to a particular vendor's electronic remote access ~~session~~. The obligation in Section 6.1 requires that entities have a method to determine ~~active~~electronic vendor remote access ~~sessions, R2 requires that said method be documented and implemented~~.

[1] ~~Similar to CIP-013, the term *vendor(s),* as used in the standard, is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.~~

[2] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[3] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

~~In support of Attachment 1 Section 6.3, and in line with FERC Order No. 829 (p.49), increased vendor remote access visibility may give Responsible Entities the ability to rapidly disable remote access sessions in the event of a system breach.~~

Attachment 1 Section 6 Part 6.2 – ~~Detecting known or suspected malicious communications for both inbound and outbound communications~~Disabling vendor remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to ~~detect known or suspected malicious communications such that the entity may respond to and remediate resulting impacts. The obligation in Section 6.2 requires that entities which allow vendor remote access (including interactive remote access) must establish a process/procedure to detect malicious communications from vendors and the systems used by vendors to access low impact BES Cyber Systems. R2 requires that these methods be documented and implemented.~~

~~Attachment 1 Section 6 Part 6.3 – Disabling vendor remote access~~

~~The objective of Attachment 1 Section 6.3 is for entities to have the ability to disable active remote access sessions in the~~disable electronic vendor remote access in the event of a security event ~~of a system breach as specified in Order No. 829 (P. 52). Per FERC Order 829 (p.49),~~, the inability of a responsible entity to ~~rapidly~~ terminate a connection may allow malicious or otherwise inappropriate communication to propagate, contributing to a degradation of a BES Cyber Asset's function. Enhanced visibility into electronic vendor remote ~~communications~~access and the ability to ~~rapidly~~ terminate ~~a~~electronic vendor remote ~~communication~~ access could mitigate such a vulnerability. The obligation in Section 6.~~3~~2 requires that entities have a method to disable ~~active~~electronic vendor remote access ~~sessions, R2~~.

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications by vendors, such that the entity may respond to and remediate resulting impacts. This sub part is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that ~~said method(s)~~ entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with low impact BES Cyber Systems.

Current Requirements in CIP-003-8 R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact BES Cyber Systems and medium impact BES Cyber Systems. Security controls such as use of intermediate systems and multi-factor authentication provide high impact BES Cyber Systems and medium impact BES Cyber Systems additional security from malicious communication and overall access controls. In addition to Intermediate Systems and multi-factor authentication, high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be ~~documented and implemented.~~ a scenario where a vendor directly communicates with a Low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security Requirements to detect malicious communications under CIP-003-X Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2020-03 Supply Chain Low Impact Revisions

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-003-X. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement
VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations
Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-003-X, Requirement R1
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-003-X, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was modified by adding a seventh topic to Requirement R1.2 for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to review one or more documented cyber security policies covering the topics specified in Requirement R1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-X, Requirement R2

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2)	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber	plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
implemented electronic vendor remote access security controls but failed to document its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR	implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic vendor remote access security controls, but failed to implement electronic vendor remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		

VSL Justifications for CIP-003-X, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The attachment to Requirement R2 was modified by adding a sixth section for topics that should be included in documented cyber security policies for assets identified in CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect six topics instead of five that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented cyber security plans covering the sections specified in Attachment 1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-X, Requirement R3
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R3
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VRF Justification for CIP-003-X, Requirement R4
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R4
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Extended, Now Open through April 15, 2022

Now Available

The 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls** has been extended and is now open through **8 p.m. Eastern, Friday, April 15, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Commenting
Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps
An additional ballot for the standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 6-15, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions (Draft 2)
Comment Period Start Date:	2/25/2022
Comment Period End Date:	4/15/2022
Associated Ballots:	2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 2 ST

There were 75 sets of responses, including comments from approximately 167 different people from approximately 114 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the updated language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Santee Cooper	Chris Wagner	1		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC
					LaChelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Paul Camilletti	Santee Cooper	1,3,5,6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO

					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool,	2	MRO

						Inc.		
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
LaKenya VanNorman	LaKenya VanNorman		SERC	Florida Municipal Power Agency (FMPA)	Chris Gowder	Florida Municipal Power Agency	5	SERC
					Dan O'Hagan	Florida Municipal Power Agency	4	SERC
					Carl Turner	Florida Municipal Power Agency	3	SERC
					Richard Montgomery	Florida Municipal Power Agency	6	SERC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy	3	RF

						Corporation		
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC

Helen Lainis	IESO	2	NPCC
David Kiguel	Independent	7	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability	10	NPCC

						Council		
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Portland General Electric Co.	Ryan Olson	5		PGE Group 2	Brooke Jockin	Portland General Electric Co.	1	WECC
					Dan Zollner	Portland General Electric Co.	3	WECC
					Daniel Mason	Portland General Electric Co.	6	WECC
					Ryan Olson	Portland General Electric Co.	5	WECC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable

					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC Entity Monitoring	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. Do you agree the updated language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT align the CIP-003 Attachment 1 Section 6 language with CIP-005-6 R2 and use NERC-defined terms where possible. The content of Section 6 should be included within Attachment 1 Section 3 and not made into a new section. Reclamation recommends adding “if technically feasible” to Section 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

Reclamation recommends the following changes to Section 6:

From:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

To:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including **Interactive Remote Access** and system-to-system **remote** access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for **identifying active** vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling **active** vendor remote access.

The phrase “determining active vendor remote access sessions” is not clear. Reclamation recommends using the same language as in the Technical Rationale, which refers more specifically to ”when sessions are initiated.”

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

As with the previous draft, Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS. Section 6.3 would require detection of malicious inbound and outbound communications for low impact BCS with vendor remote connectivity. In the current version and next effective version of CIP-005, Part 1.5 requires detection of malicious inbound and outbound communications only for medium impact BCS at **Control Centers**.

The Technical Rationale points out that Mediums already have other requirements ("use of intermediate systems and multi-factor authentication") which can be used to PROTECT against malicious communication; however, none of those requirements specifically require that entities DETECT malicious communication at Mediums. Until this gap is fixed, entities will be expected to detect malicious communications at certain of their Low assets but none of their Medium assets outside of a control center.

In addition, BPA is concerned that by not properly limiting the scope statement for Section 6 to sites with vendor remote access, we may have to prove a negative.

BPA recommends the following ***revision***:

Section 6. Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) ***with vendor remote access*** identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include…

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

The introduction of "detecting known or suspected malicious communications" for low impact BES Cyber Systems would be more stringent as compared to CIP-005 R1.5 since Medium Impact BES Cyber Systems are not applicable in the current version of the standards without adding any additional reliability benefits.

Likes 0	
Dislikes 0	
Response	

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy feels Attachment 1 Section 6.3 is not clear in its intention of the standard and obligation of industry. We feel Attachment 1 Section 6.3 needs to be drafted to be as clear as 6.1 and 6.2	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
PNM supports the EEI inclusion of the word “active” in 6.1 and 6.2. However, with the inclusion of the word “active”, the current proposed language in 6.1 and 6.2 which reads, “where such access has been established under Section 3” may be redundant. PNM supports EEI comments regarding 6.3 to more specifically narrow the scope of detecting known or suspected malicious communications for both inbound and outbound “electronic vendor remote access, where such access has been established under section 3.”	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	No
Document Name	
Comment	
Refer to NAGF comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #1.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the opportunity to reeview and provides the following comments.

BC Hydro's assessment is that the language proposed in CIP-003-X attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- The language used in CIP-003-X attachment 1 Section 6.3 is referring to 'known or suspected malicious communications'. BC Hydro recommends adding more clarity and provide examples of use cases and applicability. Specifically, context and usage of the term 'malicious communication' needs more clarity and BC Hydro requests to provide the context and usage with pertinent examples and use case scenarios to improve understanding and to better scope the requirements.
- Similarly, BC Hydro proposes defining and adding the term 'Electronic Vendor Remote Access' to NERC Glossary of Terms
- Bc Hydro also suggests that who and what is to be considered a 'Vendor' needs to be defined in the Glossary of Terms for clarity.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote access; however, this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.3 completely.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No

Document Name	
Comment	
For this question we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	

NextEra Energy respectfully submits the following language changes to Attachment 1 and Attachment 2 replacing “electronic vendor remote access” with “Vendor Electronic Remote Access” for consistency and clarification.

Consider the following language:

x Attachment 1

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with **vendor electronic remote access**. These processes shall include:

6.1 One or more method(s) for determining **vendor electronic remote access** where such access has been established under Section 3;

6.2 One or more method(s) for disabling **vendor electronic remote access** where such access has been established under Section 3; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications **supporting vendor electronic remote access**.

CIP-003-x Attachment 2

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 to mitigate risks associated with **vendor electronic remote access** may include, but are not limited to:

1. For Section 6.1, documentation showing **method(s) for determining vendor electronic remote access where such access has been established under Section 3 that may including the following:**

- steps to preauthorize access;
- alerts generated by vendor log on;
- session monitoring;

- Security Information Management logging alerts;
- time-of-need session initiation;
- session recording;
- system logs; or
- other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing **method(s) for disabling vendor electronic remote access where such access has been established under Section 3 that may including the following**:

- disabling **vendor electronic remote access** user or system accounts;
- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active **vendor electronic remote access;**
- disabling communications protocols (such as IP) used for systems which establish and/or maintain active **vendor electronic remote access**;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active v**endor electronic remote access**; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of **method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor electronic access communications that may including the following**:

- Firewall policies;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;
- manual log reviews; or
- other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	No
Document Name	

Comment

Anything prompting action at the low impact level must be very succinct otherwise risk overwhelming already taxed resources devoted to cyber security. More detail must be developed to limit the scope of communications that will be covered.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachement 1 Section 6 more closely resemble the language as written in the NERC Board resolution and the CIP-005 Standard.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The NAGF previously recommended that the SDT align the language to include the word "active", which is utilized in both the Board Resolution and CIP-005 R2.4. The NAGF is concerned that using the word "electronic" may cause a differing definition and expectation to be developed over time compared to the objective of the language in the Board Resolution. Does the SDT view "active" and "electronic" as synonymous terms? If the SDT does not see "active" and "electronic" remote vendor access as synonymous further definition of "electronic" is required.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment
LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachement 1 Section 6 more closely resemble the language as written in the NERC Board resolution and the CIP-005 Standard.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
EEI recognizes that the proposed changes under this project are intended to align with the NERC Board resolution, however, EEI is concerned that the proposed Draft 2 language in Attachment 1, Section 6 goes beyond the intent of the Board resolution by being overly broad. In addition, the proposed language in Section 6 is not risk-based and could be understood to mean all low impact BES Cyber System communications are included. As a result, entities would be faced with difficult choices that include how to safely allocate scarce resources (i.e., limited budgets and qualified SMEs) to meet existing CIP-003 requirements while also covering the unfettered expansion of low impact BES Cyber System communications. To address this concern, we ask that the SDT employ a risk-based approach that allows entities to develop processes that focus their resources on those systems that represent known risks. In addition to the above concern, EEI supports the proposed language in Section 6, subparts 6.1 and 6.2 but suggests some minor edits as indicated in the bold text below. In particular the proposed language for subpart 6.3 is not sufficiently aligned with communications as established under Section 3. The introduction of the new undefined term “vendor communications” needs additional explanation or clarification because it is treated separately and not aligned with Section 3. For these reasons, we recommend adding the text in bold to define the scope more clearly. **Section 6**: Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible entity shall implement a process to mitigate risks associated with electronic vendor remote access. These process shall include: 6.1: One or more method(s) for determining **when active** electronic vendor remote access **has been initiated**; where such access has been established under Section 3; 6.2: One or more method(s) for disabling **active** electronic vendor remote access **when necessary;** where such access has been established under Section 3; and 6.3: One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound **electronic** vendor **remote access, where such access has been established under Section 3**.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	
Comment	
Based on the comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The language used in of the NERC Board resolution states the CIP-003 is “to include policies for low impact BES Cyber Sytems…”. We agree with the SDT’s interpretation that 3 controls listed in the resolution should be addressed not only in the CIP-003 R1.2, policies but in the plans required in CIP-003 R2 and Attachment 1. While the R2 additions are an expansion beyond the NERC Board resolution, they are required to meet the intent of the resolution. Because CIP-003 Attachment 1 is written to apply at the “assets containing low impact BES Cyber Systems” and not to just the “BES Cyber Systems”, the 3 controls listed in the NERC Board resolution could be required to be applied to more than low impact BCS. This expansion in scope beyond low impact BCS is not required by the NERC Board resolution. The expansion could include additional controls being required for medium and high impact Cyber Assets beyond what are included in as “Applicable Systems” in CIP-005 R1.5 and R3. Regarding the control concerning malicious communication, we feel that this should be limited to only low impact BCS at Control Centers to align with CIP-005 R1.5. An interpretation of what the SDT has proposed could require the detection of malicious voice communication, text messages, or emails from anyone to anyone that is at an asset containing low impact BES Cyber Systems. The NERC Board resolution includes the implementation of controls to “disable active vendor remote access.” CIP-005 R2.5 addresses disabling active vendor remote access and R3.2 addresses terminating vendor initiated remote connections. The actions listed in Attachment 2 and the language used in the Technical Rational for Attachment 1 Section 6 Part 6.2 combine disabling and terminating as part of the required control. The SDT should limit the scope to disabling active vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.	
Likes 0	
Dislikes 0	

Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term “vendor communications” needs explanation.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electrical Institute’s (EEI) comments and believes the drafted language more adequately addresses the purpose/goal as stated in the SAR and Technical Rationale	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	No
Document Name	
Comment	
FMPA supports comments from Utility Services, Inc.	

Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
Portland General Electric Company (PGE) supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST notes that the NERC BoT's resolution, as written, does not explicitly limit the application of a malicious code detection requirement to remote connections to or from vendors.	
Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
While we agree with the updated language as a whole, we support EEI’s proposed modification to Attachment 1 Section 6, as it adds clarity.	
Likes 0	
Dislikes 0	

Response

Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted : “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.	
Likes 0	
Dislikes 0	
Response	

Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments below: ACES Comments: While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted : “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NERC Standards Review Forum (NSRF) agrees proposed language addresses the risk.	

Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
We agee because this gives the ability to disconnect, we ask the drafting team to include examples of evidence for this requirement (log ins?).	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	

Response	
Brian Lindsey - Entergy - 1	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted : “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form.docx
Comment	
While GSOC agrees that the proposed language addresses the risks identified by the NERC Board Resolution, it is concerned that the absence of the term “active” broadens this requirement beyond the obligations set forth to manage vendor access for medium and high impact BES cyber assets. In particular, the language of the similar requirements for vendor access management in CIP-005-7, R2.4 and R2.5 focuses the requirements on	

determining and disabling “active vendor remote access sessions.” The language proposed in Attachment 1, Sections 6.1 and 6.2, however, could be interpreted to apply to any authorized vendor remote access – regardless of whether or not the vendor has initiated or is in an active remote access session.

Such a requirement would result in low impact BES cyber assets being subject to more stringent security controls than high or medium impact BES cyber assets and appears to conflict with the Technical Rationale for these sections as provided on page 5 of the proposed Technical Rationale document. To ensure that the security controls applied to low impact BES cyber assets are commensurate with risk and not more stringent than those applied to high and medium impact BES cyber assets, GSOC recommends that the SDT mirror the language provided in CIP-005-7, R2.4 and R2.5 to the extent possible. For example, revisions could be made as follows:

For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include:

6.1 One or more method(s) for determining active electronic vendor remote access sessions where such access has been established under Section 3;

6.2 One or more method(s) for disabling active electronic vendor remote access where such access has been established under Section 3; …

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas Re appreciates the SDT and NERC legal looking into the issue of whether or not Part 1 of the NERC resolution has been satisfied. Texas RE suggests the SAR and the report do provide flexibility for the SDT to consider language for detecting known or suspected malicious communications for all inbound and outbound communications, and not be limited to vendor inbound and outbound communications. Texas RE continues to recommend the SDT clarify that CIP-003 low impact monitoring obligations extend to all inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of vendor remote access. Texas RE notes this approach is consistent with FERC's January 20, 2022 Notice of Proposed Rulemaking (NOPR) regarding internal network security monitoring.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	

Comment
Xcel Energy agrees that Attachment 1 Section 6 addresses the risk malicious communication posed by vendors accessing low impact BES cyber systems from remote locations. However, there is a lack of clarity of which types of cyber assets are in scope for subpart 6.3. Xcel Energy suggests that language of "as established in section 3" be added to section 6.3 as it is in sections 6.1 and 6.2.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	

Comment
No comment.

Likes 0	
Dislikes 0	

Response

2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Header 6.1 and 6.2 - Add the word “active” in the requirement and move “electronic” adjective. One or more method(s) for determining *active* vendor *electronic* remote access where such access has been established in Section 3.	
Likes 0	
Dislikes 0	
Response	

Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST suggests dropping "electronic" from the phrase, "electronic vendor remote access." The only kind of remote access to electronic devices (including Cyber Assets) that presently exists is electronic. In addition, NST believes the remote access terms the SDT has used in CIP-003 Sections 6.1, 6.2 and elsewhere should be consistent with the language in CIP-005, which addresses "vendor remote access," not "electronic vendor remote access." Consistent use of terms enables Responsible Entities with assets other than low impact to develop and apply controls across assets of differing impact levels.	
Likes 0	
Dislikes 0	

Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	

Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electric Institute's (EEI) comments. Draft 1 of Attachment 1 Section 6 included the clarifying language "(including interactive and system-to-system access)" which was removed from Draft 2, making it unclear what forms of access are in scope. Additionally, the term "vendor" is an undefined term and should be clarified in the NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelon doesn't agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelon doesn't agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats	

internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

The SDT has used the word “electronic vendor remote access” and not the term “active vendor remote access” that is used in CIP-005-7 and in the NERC Board resolution. It is unclear why this inconsistency is needed or what the difference is between the two terms.

Furthermore when reviewing the Technical Rationale behind these proposed modifications, a footnote which had previously referenced guidance on the term “vendor” and how it may be used in the current version of CIP-013 and the future versions of CIP-005, CIP-010, and CIP-013, had been removed making for more confusion on what a vendor may be in this scope. Can the SDT please provide the reasoning for removing the footnote/reference from the Technical Rationale?

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Recommend using the CIP terms “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
More work should be undertaken to clearly define the terms remote access and the scenarios.	
Likes 0	
Dislikes 0	
Response	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	
Generally “interactive” remote access is also used. Interactive means not only read only or view only access. This should be a part of the standard as if I am only viewing or retrieving read only data there is no ability for the remote connection to make changes or perform actions.	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	
Please see NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No

Document Name	
Comment	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As mentioned in comments related to Question 1 above, ' Electronic Vendor Remote Access' needs additional clarity to ensure proper understanding of applicability as well as the use of term 'Vendor' e.g., whether consultant using same infrastructure is considered vendor?	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #2.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No

Document Name	
Comment	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
PNM supports EEI comments regarding the needed clarity around “remote access” referring to user remote access, machine remote access, or both.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy agrees with EEI’s comments: “While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.”	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No

Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP would like to see “Electronic Vendor Remote Access” as a clearly defined term. For example, is web-conferencing considered electronic vendor remote access?	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.”	
Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment
Southern Indiana Gas and Electric (SIGE) does not believe that this language is clear or widely used. The most widely used description of remote access is interactive remote access. If the SDT intends to include system-to-system access then that should be made clear. Remote access should be clearly defined as interactive access and system-to-system remote access. SIGE proposes re-installing the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, “(including interactive and system-to-system access) to low impact BES Cyber Systems.”

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
Remote access should be clearly defined as including interactive and system-to-system remote access. CenterPoint Energy Houston Electric (CEHE) proposes re-instating the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, “(including interactive and system-to-system access) to low impact BES Cyber Systems.”

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	

Comment
If “remote access” is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the “Interactive Remote Access” definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	
Comment	

Reclamation recommends adding “Vendor” to the NERC Glossary of Terms and proposes the following definition:

Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts to supply equipment for BES Cyber Systems and related services. Vendor does not include other NERC-registered entities that provide reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). Vendor may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	
Comment	

If “remote access” is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the “Interactive Remote Access” definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.

Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	
Comment	

GSOC agrees that remote access is a widely used and understood term and would suggest that the language used in Attachment 1 more closely mirror the language utilized in CIP-005-7 to reduce the potential for additional confusion, ambiguity, and subjective interpretation. Please see comments provided in response to question 1 above.

Likes 0	
Dislikes 0	

Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes that the term "remote access" is commonly used to address electronic access originating from locations outside of protections established in an entities PSP and ESP.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
We believe that the language is clear.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

Comments: Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a "remote location".

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a "remote location".

Likes 0	

Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	

Comment
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	

Comment
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment
BC Hydro suggests that the use of word "Remote" will need clarification and perhaps a definition in the Glossary of Terms. For example, in the scenarios below, how will the "Remote" term be used? 1. On site, but electronically remote (i.e. has to go through EAP despite being at the station).

2. A "vendor" at the work location of Responsible Entity, also electronically remote (i.e. going through EAP).
3. "Traditionally" remote, off site, and electronically remote (also going through EAP).

Likes 0	
Dislikes 0	

Response

Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1

Answer	No
Document Name	

Comment

Please see NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The NAGF membership is concerned with the "remote locations" language in this question. Remote location is not used to describe the vendor's access in any version of the standard language. Is the SDT referencing geographic location or network topology? The standard language references inbound and outbound communications between the BES Cyber System and "Cyber Asset(s) outside the asset" (Section 3.1.i).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at

the system level while Low controls are at the asset level.

Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

We disagree that the intent of the NERC Board resolution is to address vendor access to low impact assets. Our understanding of the NERC Board resolution is that the controls are to apply to low impact BES Cyber Systems at assets that have low impact BES Cyber Systems. The SDT's interpretation could require the 3 controls to be applied to vendor remote access and communication to more than not just low impact BCS.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon ultimately believes this would require us to have an inventory list of the lows impact assets.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon believe that ultimately, this would require us to have an inventory list of the lows impact assets.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
The new undefined term “vendor communications” needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using “active” electronic vendor remote access and in 6.3 add “…where such access has been established under section 3”	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
The new undefined term “vendor communications” needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using “active” electronic vendor remote access and in 6.3 add “…where such access has been established under section 3”	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

"Vendor communications" is a new term. It doesn't scope this new term to communications "as established in Section 3" as the others do. "Vendor communications" is too broad of a term and wide open to many interpretations of the definition meaning.

Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Yes, the SDT has clarified the scope.

Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy belives the scope is clear.	
Likes 0	
Dislikes 0	

Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #3.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	

Brian Lindsey - Entergy - 1	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees in part that the language in Attachment 1, Section 6 is clear but offers some suggested edits for SDT consideration. (See our response to Question 1)	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	

Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Although NST agrees Section 6 applies only to vendor remote access, it is our opinion that a malicious code detection requirement should not be limited to only vendor remote connections.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal	

Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
Vendor remote access needs to be clear to convey remote access only	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Deanna Carlson - Cowlitz County PUD - 5

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

6.3 language needs to be clearer and have a tighter bounded scoping to avoid the widest possible interpretation at audit. You can't go to Section 3 Electronic Access Controls evidence and show you are detecting things on all identified LERC and fully prove 6.3 as it is currently written. The intent of 6.3 should be added as a requirement to Section 3.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6

Answer	No
Document Name	

Comment

PGE supports the survey response provided by EEI.

Likes 0	
Dislikes 0	

Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that has a low.	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that has a low.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that contain lows.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelons interpretation of the proposed standard views that this opens up access to ‘any’ areas that has a low	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The proposed language in Section 6.3 could be interpreted to include communication to people and all Cyber Assets at an asset that contains low impact BCS. The controls for active vendor remote access could also be required to be applied to all Cyber Assets at the asset and not just those that are part of a low impact BCS. We would suggest appending a statement consistent with the other two subsections of Section 6, “where such access has been established under Section 3.”	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI disagrees that the language in Attachment 1, Section 6 clearly limits the scope to low impact BES cyber systems. While we agree with the changes	

made to Section 6, subparts 6.1 and 6.2; the proposed language in subpart 6.3 is not sufficiently narrow. (See our response to question 1 above.)

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

LCRA believes that the current wording makes it unclear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

LCRA believes that the current wording makes it clear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	No
Document Name	

Comment

much more work is needed to sufficiently scope the low impact assets which will be considered in scope.

Likes 0	
Dislikes 0	
Response	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	
Clarity is needed for when low impacts systems exist in conjunction with medium impact systems located at Medium BES Assets/Facilities. I.E. situations where there is a medium impact BES Asset/Facility that also contains low impact systems.	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	
Please see NEE’s response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.3 completely.	

Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #4.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Section 6.3 should either reference Section 3.1 or somehow limit to only low impact BES cyber systems.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy believes additional clarity could be established by adding verbiage to 6.3 that includes "as established in section 3"

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	No
Document Name	

Comment

See EEI comment.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1

Answer	No
Document Name	

Comment

Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	No
Document Name	

Comment

The inclusion of 'where such access has been established under Section 3' appears to bring into scope electronic vendor remote access to Cyber Assets that **are not** low impact BES Cyber Systems, but on the same network as a low impact BES Cyber System based on the language of Section 3.1 ii 'using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).' This is due to the fact that CIP-003 uses 'asset containing' as a boundary.

Please consider the following two options –

Option 1: Scope Section 6 specifically to Section 3.1 i, which would more accurately scope to only low impact BES Cyber Systems.

Section 3.1 i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

Option 2: Do not reference Section 3 or any part thereof, but include the following language in Attachment 1 Section 6 –

'between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).'

6.1 One or more method(s) for determining electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside

the asset containing low impact BES Cyber System(s);

6.2 One or more method(s) for disabling electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside asset containing low impact BES Cyber System(s); and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

There is confusion with the language used in Section 6 as to whether it pertains to the assets containing the low impact BES Cyber Systems (which may contain out of scope cyber systems) or the low impact BES Cyber Systems themselves.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP believes the proposed changes to the CIP-003 Standard are trending in the right direction overall, there was language struck through that we think adds clarity to the scope of the section. The aforementioned struck through language in Attachment 1 Section 6 is in bold below:

Section 6: Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access **(including interactive and system-to-system access) to low impact BES Cyber Systems that includes:**

To provide a more clear understanding that the language in this section limits scope to low impact BES Cyber Systems, AEP recommends reinstating the language above that was struck from this revision.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The lack of specificity in the “access to low impact BES Cyber Systems” verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, “assets containing low impact BES Cyber System(s)” which does not limit the scope to only the “low impact BES Cyber Systems”. If the intent is to limit the scope to “low impact BES Cyber Systems” and not the “assets containing low impact BES Cyber Systems”, then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.

Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Comments: The lack of specificity in the “access to low impact BES Cyber Systems” verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, “assets containing low impact BES Cyber System(s)” which does not limit the scope to only the “low impact BES Cyber Systems”. If the intent is to limit the scope to “low impact BES Cyber Systems” and not the “assets containing low impact BES Cyber Systems”, then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
While NST agrees the Section 6 language limits the scope to low impact BCS, it is our opinion that it does not adequately define the types of in-scope vendor remote access. Do Sections 6.1 through 6.3 apply to vendor remote access via dial-up? Rather than simply use a blanket referral to Section 3 in Sections 6.1 and 6.2, Section 6 should refer to specific sub-parts of Section 3 (e.g., Section 3.1, Part i).	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
No additional comments	

Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	

Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes, the SDT has made the scope clear.	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

Comments: Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

The examples provided support what is required in Attachment 1 Section 6. Clarification in the language used is suggested, along with an additional example for vendor machine to machine remote access:

Electronic Vendor Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation **AND EVIDENCE OF IMPLEMENTATION** showing:

 DOCUMENTED steps to preauthorize access **ALONG WITH AUTHORIZATION RECORDS**

 CONFIGURATION OF alerts generated by vendor log on;

 PROCEDURES FOR THE USE OF VENDOR session monitoring **AND SESSION MONITORING LOGS**;

 Security Information Management logging alerts; **- REDUNDANT TO #1, CAN BE REMOVED**

 DOCUMENTED STEPS AND LOGS FOR time-of-need session initiation;

 DOCUMENTED STEPS AND LOGS FOR VENDOR REMOTE ACCESS session recording;

 DOCUMENTATION AND CONFIGURATION OF system logs **SHOWING VENDOR REMOTE ACCESS CONNECTIONS**

 DOCUMENTATION OF ELECTRONIC ACCESS CONTROL RULES PERMITTING INBOUND VENDOR MACHINE TO MACHINE COMMUNICATION; or

 other operational, procedural, or technical controls.

For Section 6.2, documentation showing **THE PROCESS FOR:**

 disabling vendor remote access user or system accounts;

 disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;

 disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;

 Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);

 administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access; or

 other operational, procedural, or technical controls.

For Section 6.3, documentation showing implementation of:

 Firewall policies **IMPLEMENTING MALICIOUS TRAFFIC INSPECTION**;

 Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);

 Virtual Private Network (VPN) hosts **IMPLEMENTING CONNECTION INSPECTION**;

 manual log reviews; or

 other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Not clear if VPN connections established with support vendors fully adheres to requirement or additional steps are required such as an IDS/IPS.	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet –	

“administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.” Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – “Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).”	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.”	
Likes 0	
Dislikes 0	
Response	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	
Additional ephasis should be put on Programmatic non technical methods of allowance to clarify that processes can be leverage rather than purely technical methods.	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – “administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access.” Attachment 1, Section 6 does not say “active vendor remote access.” Next, that bullet is inconsistent with the first Attachment, 6.2 bullet – “disabling vendor remote access user or system accounts.” Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – “Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).”	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Firewall Policy and Virtual Private Networks aren’t the greatest examples of capturing whats in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	No
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	No
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.

Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes, the examples support our understanding of what is required.	
Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	

Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	

Comment
Attachment 2 Section 6 includes multiple uses of 'vendor remote access' and 'active vendor remote access.' To ensure a consistant scope to Section 6 consider changing all to '***electronic vendor remote access***.' disabling ***vendor remote access user*** or system accounts disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN,Remote Desktop, remote control, or other hardware or software used for providing ***active vendor remote access*** disabling communications protocols (such as IP) used for systems which establish and/or maintain ***active vendor remote access***; administrative control documentation listing the methods, steps, or systems used to disable ***active vendor remote access***;

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	

Comment
See EEI comment.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	
Comment	
Xcel Energy believes that examples in Attachment 2 provide clarity to what is required in demonstrating compliance with Section 6.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State mostly agrees however, the example of Steps to Preauthorize is confusing and too open-ended.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #5.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment	
The MRO NSRF believes that the example are clear.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI agrees that Attachment 2, Section 6 examples support what is required under Attachment 1, Section 6.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC recommends that the language in Section 6.1 be revised to more closely mirror the language of CIP-005-7, R2.4, which would more clearly indicate the time frame and intent/activities to which the requirement and documentation should be focused.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

The examples listed for Section 6.2 include controls for disabling and controls for terminating remote access. In addition, these examples use the terms “vendor remote access” and “active vendor remote access” but do not use the “electronic vendor remote access” term used in Attachment 1. While we do not think the term “electronic vendor remote access” should be used at all, there should be consistency throughout the document and preferably, consistency throughout the CIP Standards.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

No additional comments	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST has no comment.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes that a considerable amount of research would be needed before many respondents would be able to provide a well-informed answer to this question. We note the December 2019 “Supply Chain Risk Assessment” report states, “More than 99% of the responders (to a survey question about costs and benefits) agreed with the draft response that it was premature for CIP-013 registered entities to determine or estimate costs or benefits associated with the implementation of the standard…” That said, NST believes the cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3 and on the number of facilities where controls may need to be applied.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Until additional clarity is provided on the scope and intent of the proposed modifications, the overall cost is difficult to ascertain.

Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.	

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The expansion of the requirement to detect suspicious malicious communication to systems that may not have routable communication and to systems that are not at a Control Center, as is required for high and medium impact, imposes costs that are not consistent with the risks as determined by previous Standard Drafting Teams. Furthermore we believe the SDT is only accounting for the cost of the equipment that would be responsible for performing the tasks of Section 6. While this is one cost to consider, there may be additional resources required to allow for implementation of such technology including but not limited to additional staffing, training, or other equipment that would allow a SIM/SEM/SIEM or IDS/IPS to have visibility.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	

Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal challenges to entities.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

This is very dependent on how an entity chose to implement it’s low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal

challenges to entities.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
Any low impact related changes are likely to lead to significant scope creep and potentially many underlying, unknown costs that will be incurred.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	

Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The MRO NSRF has concerns about the potential of ineffective costs. Due to recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors the cost of implementation of the Requirements is at a much higher risk than what would normally be expected. Higher than expected costs may result in the need for a longer or adaptive implementation timeline.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment
Although the cost may differ between entities, BC Hydro's assessment is that the impact may change based on understanding & clarity of terms and scope of application. As outlined in BC Hydro's comments to Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However, the requirement in CIP-003-X Section 6.3 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5, where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS out of scope. Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	

Comment
Making this a requirement on all low impact BES Cyber Systems would be extremely expensive because new equipment must be installed at each low location to monitor for remote vendor access, allow for the ability to terminate sessions and detect malicious code. It would be more cost effective to create a risk-based approach that would target those low impact BES Cyber Systems that could have the most potential impact on the BES.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
There are many entities that have a large amount of low impact sites that are in remote locations and struggle with limited bandwith that will be impacted. With the recent supply chain and staffing issues you will have higher than normal costs to implement these requirements.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	

Comment
Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	

Comment
Xcel Energy is concerned with meeting the demands of section 6 in a cost effective manner at this time. World events have created issues with supply chain and receiving the needed products to perform activities required in the standard in a timely and cost effective manner. The vast number of low impact sites as compared to high and medium sites will cause a sudden surge in demand and cause prices to rise dramatically. The standard drafting team should take these issues into consideration in their implementation plan to spread costs and demand for products across and longer span of time.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment
AEPCO is signing on to ACES comments below. ACES comments: This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.

Likes 0	
Dislikes 0	

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer	No
Document Name	

Comment
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No

Document Name	
Comment	
This is very dependent on how an entity chose to implement it’s low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

Depending on the solution(s) determined by NIPSCO, cost would most likely be a factor to purchase the equipment and resources necessary to achieve the goal of securing vendor remote access.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The scope should be narrowed to just where the risk exists as opposed to a broad swath of assets. The way it is written it implies that all communications need to be monitored to determine malicious communications through vendor remote access.

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No
Document Name	

Comment

Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003

Attachment 1 requirements and prove detrimental to a cost-efffective approach. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends this project may be a good avenue to incorporate low impact requirements into these standards to avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Comments: These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003 Attachment 1 requirements and prove detrimental to a cost-efffective approach. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC is concerned that compliance with Section 6, as proposed, may require a significant investment of resources, specifically that such investment is beyond what is applied to protect high or medium impact BES cyber assets despite the fact that such investment may not yield commensurate reliability and security benefits.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	

No comment.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

GO/GOPs will need more information to adequately assess the cost-effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4

Answer	
Document Name	

Comment

We will need more information to adequately assess the cost-effectiveness of the proposed approach

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form_02252022 Presentation FINAL COMMENTS v2.docx
Comment	
To be “cost effective”, this implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change. Additional staff and procedures will be required to monitor this level of detail to meet the requirements of CIP-003.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on the question.	
Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
SIGE will not provide a response to the cost effectiveness of the proposed changes to CIP-003-x.	

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
A longer implementation timeline would offer more cost effectiveness. This would allow industry to spread their investments and capital purchases.	
Likes 0	
Dislikes 0	
Response	

7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel/vendors appropriately.

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No
Document Name	

Comment

BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: “If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity.” While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Sections 6.1 and 6.2 will not have equivalent language for Mediums without ERC until CIP-005-8 R2.4 and R2.5 are adopted. Therefore, BPA recommends that implementation of these sections should be aligned with the passage of CIP-005-8 to avoid entities having to monitor their Low assets but not their Mediums without ERC and/or Dialup.

Section 6.3 has no current equivalent language in CIP-005-8 (nor any other standards) for Medium impact BES Cyber Systems except at Control Centers. Until then, entities will be expected to detect malicious communications at certain Low assets but none of their Medium assets outside of a control center. This is a significant gap; BPA recommends that the drafting team delay Section 6.3 until CIP-005 is expanded to include Mediums outside of Control Centers.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	

Comment

After further consideration, we believe that a 36 month implementation timeline would be most appropriate for incorporating all the revisions in Project 2020-03. This will allow for proper installation, testing and documentation of new controls across a large inventory of sites and assets. This timeline would also be more feasible given the current supply chain challenges across industry.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The expansion of scope for vendor remote access monitoring and malicious communication monitoring may require new technology to be implemented within the program. The implementation for said technology for a large utility will require a longer implementation than 24 months.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
36 months minimum as additional staff or staff augmentation would have to be employed as there would be a significant amount of design, planning, testing, and finally, deployiment of solutions to the affected assets in the field.	
Likes 0	
Dislikes 0	
Response	

Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS feels that a 24-month implementation plan would be a reasonable timeframe to implement process, procedures or technology to meet the proposed language in Sections 6.1 and 6.2, in addition to Section 6.3. It may be necessary to design and implement multiple solutions to meet the proposed language in Section 6 across the various environments in which low impact assets are in use. Alternatively, a single solution which could be applied across a broader group of low assets may require significant design changes to process, procedures and/or technology.	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Due to supply chain constraints on security equipment we believe an additional 12 months should be included or an exception were procurements happens within that time frame to adhere compliance.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: “If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity.” While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
A 24 month implementation is desirable due to budget, supply chain, and resources to implement solutions for SRP’s Generation fleet.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Section 6.3, to allow entities more time to implement, the required control, if necessary.	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES comments: Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Setion 6.3, to allow entities more time to implement, the required control, if necessary.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	

PNM supports EEI comments regarding the implementation timeframe for 6.3 to be extended to 36-months if the scope of 6.3 is not sufficiently narrowed as mentioned in the comments for question 1.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy is concerned with meeting the implementation demands of section 6 within the proposed timeline identified in the implementation plan. World events have created issues with supply chain and obtaining the needed products and staff to perform activities required in the standard in a timely manner. The vast number of low impact sites as compared to high and medium sites will cause a sudden surge in demand and cause prices to rise dramatically. Additionally, an industry-wide staffing shortage will slow efforts to implement and maintain newly procured products. The standard drafting team should take these issues into consideration in their implementation plan to spread costs and demand for products and staff across and longer span of time.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment
As mentioned in Question 6, many entities have large amount of low impact sites that are in remote locations and struggle with limited bandwith which makes procruement, and implementation of new hardware and software difficult. There is the other challenge of the recent supply chain and staffing issues that will also impact implementation timelines. The supply chain being taxed all at once by utilites to meet the short timeline should must be taken into consideration.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #7.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment
BC Hydro recommends a longer implementation plan, e.g. more than ~ 36 months considering the cost and scope impact as identified in comments to Questions 1 and 4 above. Once the clarity of terms and definitions is obtained as identified in comments to Questions 1 and 4, BC Hydro will be in a better position to provide an alternate detailed implmentation plan to meet the target completion deadline.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The MRO NSRF anticipates the procurement and implementation of new software, hardware, and associated services needed to detect vendor's malicious communications to be particularly challenging given recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors. Registered Entities across North America will all be attempting to procure needed solutions in a relatively small window of time. This will create a deficit of supply with increased demand and will drive up costs. That, along with current staffing shortages and geopolitical events, may produce scenarios that will prevent a responsible entity from meeting the effective date set in the approved implementation plan. The MRO NSRF suggests the SDT align with NERC legal staff to allow for a provision in the implementation plan that would provide an opportunity for entities to request extensions based on the aforementioned factors.

Likes 0	
Dislikes 0	
Response	

George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0	
Dislikes 0	
Response	

Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	

- NextEra Energy requests consideration of a 36-month implementation period due to a large number of sites (in the hundreds) requiring assessment and potentially new equipment and/or process implementation. The work must be planned and typically will be scheduled with planned maintenance and scheduled generation outages.

- The last few years the supply chain has adversely impacted maintenance including staffing and is expected to impact the implementation.
- Entities may need to evaluate and update vendor, supplier, customer and other agreements and contracts.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	No
Document Name	

Comment

Given the uncertainty regarding the exact scope of implementation across low impact and all vendor communications it is hard to believe the 18 months will be sufficient timing.

Likes 0	
Dislikes 0	

Response

Brian Lindsey - Entergy - 1

Answer	No
Document Name	

Comment

There could be additional needs for technology purposes which would create funding needs based on funding cycles and implementation. Strongly recommended to inceas all sections to a 24 mth implementation.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Setion 6.3, to allow entities more time to implement, the required control, if necessary.

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
EEI appreciates the two-phase implementation plan for Attachment 1, Section 6 and supports the proposed 18-month implementation plan for subparts 6.1 and 6.2. However, we do not agree that an additional 6 months to complete subpart 6.3 is adequate, particularly given the current proposed language could be interpreted to mean all low impact BES Cyber System communication. Moreover, if the current language is not narrowed consistent with a risk-based approach it may be a significant challenge for some entities to complete this work in 36 months. EEI previously noted that there will be substantial work to complete 6.3 and companies are also facing significant supply chain issues/delays to secure materials necessary to implement these changes. For these reasons, the implementation plan should be at a minimum of 36 months.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	

Comment
NVE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: “If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity.” While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. NVE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
Given the potential impact of expanded scope of Section 6.3, GSOC would respectfully request a 24 month implementation period given the current state of global supply chain lead times.

Likes 0	
Dislikes 0	

Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	

Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Until additional clarification is provided on the scope and intent of the proposed changes, it's unclear if the drafted implementation timelines are sufficient to implement the requirements.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	

Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by the Bonneville Power Administration (BPA).	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes the time required to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3 and on the number of facilities where controls may need to be applied. NST recommends a 24-month implementation time frame for all of Attachment 1, Section 6 requirements.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
We would rather have one date of 24 months for the whole thing. Simpler to track and entities are going to need the time for various reasons. Some that don't have IDS capabilities at all their sites will have to order and receive and then implement a lot of equipment at a lot of sites. The 6.1 and 6.2 can be shorter for TO/TOPs that just have substations, or for those with only control centers. With the wide diversity of vendor situations out there on everything from a small solar to a string of wind turbines to a large Generation facility and all matters of variety of vendor arrangements and support, the timeframe and implementation plan is not simple. We do not want to make the assumption that 6.3 is 'hard' and needs more time and 6.1 and 6.2 are 'easier' and can be done quicker. In some cases, it might be the opposite. Whatever the maximum implementation time is, give that to everyone.	
Likes 0	
Dislikes 0	

Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Comments: These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	

Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
If all examples in Attachment 2 are ever required then we believe that additional time above the 18 months may be required.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
The ability for entities to apply these control may be limited by the availability of equipment and the vendors qualified to install them. The SDT should request that NERC provide information on the expected number of substations that may be required to implement these controls. It may be necessary to include an automatic extension of the time allowed for implementation, if necessary, equipment and personnel to perform the installation are not available.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on the question.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
If scope of this standard is tightened to what FE believes is the spirit of the standard, we feel we could follow the proposed implementation plan. As it is written, we feel the vagueness of the draft leaves ambiguity and would require a longer implementation plan to fulfill our obligation.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

These ‘low’ requirements as written seem to be more stringent than what highs and mediums have to comply with today. Highs and Mediums have to determine ‘active’ sessions and have a method to disable remote access. That is far easier than determining what constitutes malicious inbound and outbound communications.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

NST believes it is short-sighted to add a new requirement to CIP-003 for malicious communications detection that is limited to vendor remote access only. Advocates for this limitation seem to be ignoring the possibility a Responsible Entity's own remote computer systems could be compromised by attackers and used to deliver malware to BES Cyber Systems (BCS) at BES assets containing low impact BCS. In addition, NST believes that limiting the scope of monitoring and detecting to only vendor remote access either may not be practical or may result in sub-optimal designs that would need to be updated should monitoring and detecting requirements be expanded in the future. Given the likely time, effort, and expense associated with implementing a solution for malicious code detection (using IDS or similar technology), we think it only makes sense to require it for all remote access. NST also notes that in its recent NOPR proposing "Internal Network Security Monitoring" requirements for high and medium BES Cyber Systems, FERC

indicated it is interested in the possibility of applying "INSM" requirements to low impact, as well. This suggests to us that while FERC might approve the current set of proposed supply chain revisions to CIP-003, were they to be approved by industry ballot and the NERC board, they might also direct NERC to further modify CIP-003 to apply malicious communications detection requirements to any remote access that uses routable protocols outside BES assets containing low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See Comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

See Comments submitted by the Edison Electric Institute.” with your ballot.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
SDT should consider defining the term “Electronic Vendor” in the NERC defined Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
SDT should consider defining the term “Electronic Vendor” in the NERC defined Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

What is meant by '**Electronic** Vendor'? Currently it's not a defined term, SDT should consider making this a NERC defined glossary term.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

What is meant by '**Electronic** Vendor'? Currently it's not a defined term, SDT should consider making this a NERC defined glossary term.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment

All proposed controls should be limited to only low impact BES Cyber Systems as opposed to assets containing low impact BES Cyber Systems.

The proposed control for detecting malicious communication should be limited to:

1. Only low impact BES Cyber Systems using a routable protocol to communicate across the asset boundary and,
2. Only Control Centers (to align with CIP-005-7 R1.5)

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	

Document Name	
Comment	

For future reference, request redline to last approved since that shows the true SDT proposed updates.

Recommend updating R1.2.6 by removing “Electronic” from “Electronic vendor remote access security controls.” The security concern is vendor remote access.

Recommend updating Attachment 1 by removing “Electronic” from “Electronic

vendor” for consistency with Requirement R1.2.6

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “detecting known or suspected malicious communications for both inbound and outbound vendor communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Recommend updating Attachment 2 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6

Likes 0	
Dislikes 0	
Response	

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	
Document Name	
Comment	

No comment.

Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller

Answer	
Document Name	

Comment

The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. NVE found it useful and requests that the footnote be reinstated.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

In the proposed Draft 2 of CIP-003-x, the undefined term “Electronic Vendor” has been used eleven times (including within Section 6 of Attachment 1). It is unclear what is meant by the use of this term and if this term is to remain within this Reliability Standard, the SDT should provide needed clarification through the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF membership recommends that the SDT consider providing reference architecture diagram(s) similar to previous reference model provided in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Brian Lindsey - Entergy - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	

Document Name	
Comment	

- Please provide redline to last approved since that shows the true SDT proposed updates.
- Please apply NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 to the standard and technical rationale document.
- Page 4 " The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access," change to "**The SDT agreed to retain Section 3 and establish Section 6 to address low impact vendor electronic remote access,"**
- Page 5:
- "establish and disable electronic vendor remote access." to be "**establish and disable vendor electronic remote access."**
- "low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary." to be "low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active **vendor electronic remote access** sessions are initiated; and (3) disable active **vendor electronic remote access** when necessary."
- Attachment 1 Section 6 Part 6.1 – Determining V**endor Electronic Remote Access**
- "associated with malicious communications and electronic vendor remote access." to be **"associated with malicious communications and vendor electronic remote access."**
- Attachment 1 Section 6 Part 6.2 – Disabling **vendor electronic remote access**
- Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable electronic vendor remote access." to be **"Enhanced visibility into vendor electronic remote access** and the ability to terminate **vendor electronic remote access** could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable **vendor electronic remote access**.
- Page 6
- Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications for **vendor electronic remote access**

Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

The MRO NSRF would like to thank the Standard Drafting Team, NERC Staff and all other contributors for their work on this project.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	
Document Name	

Comment

For future reference, request redline to last approved since that shows the true SDT proposed updates.

Recommend updating R1.2.6 by removing "Electronic" from "Electronic vendor remote access security controls." The security concern is vendor remote access.

Recommend updating Attachment 1 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says "detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP." 6.3 says "detecting known or suspected malicious communications for both inbound and outbound vendor communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers. The low requirement may encompass email, phone, and or mail communications from vendors, because of the vague language used.

Recommend updating Attachment 2 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6

Likes 0	
Dislikes 0	

Response
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro
Answer	
Document Name	
Comment
BC Hydro ackowledges the effort and hard work SDT put into putting these complex changes to CIP-003-X. As identified in comments to Questions 1 to 4 above. The definitions of terms and clarity of application with some specific industry use case examples will help providing a more clear understanding and likely result in a faster and appropriate approvals of these proposed changes.
Likes 0	
Dislikes 0	
Response
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster
Answer	
Document Name	
Comment
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #8.
Likes 0	
Dislikes 0	
Response
Carl Pineault - Hydro-Qu?bec Production - 1,5
Answer	
Document Name	
Comment
For future reference, request redline to last approved since that shows the true SDT proposed updates. Recommend updating R1.2.6 by removing “Electronic” from “Electronic vendor remote access security controls.” The security concern is vendor remote access.

Recommend updating Attachment 1 by removing “Electronic” from “Electronic

vendor” for consistency with Requirement R1.2.6

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “detecting known or suspected malicious communications for both inbound and outbound vendor communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Recommend updating Attachment 2 by removing “Electronic” from “Electronic vendor” for consistency with Requirement R1.2.6

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

Alliant Energy appreciates the Standard Drafting Team's work on this project.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy would like to thank the drafting team for their diligent work and bringing forward language to address the concerns identified by the NERC BOT.

Likes 0	

Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	
Document Name	
Comment	
We remain concerned that the CIP-003 Attachment 1, Section 6.3 requirement for malicious communication places a heavier compliance burden on low impact assets than High and Medium, as deliniteated in CIP-005 (2.4 and 2.5). Simply extending the the implementation timeframe for this requirement does not address that basic inconsistency.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Thank you to the SDT for their efforts and allowing AEPCO to participate in the drafting process.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
My intended vote for this ballot was negative based on the comments provided in this survey. However due to technical issues with the voting platform while casting my vote it is shown as affirmative. If possible please replace my affirmative vote with a negative vote.	
Likes 0	

Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	

Comment
See EEI comment.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	

Comment
We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Texas RE continues to have the following additional recommendations for the SDT: • Include language for (1) software integrity and authenticity, (2) information system planning and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010. • Include vendor multi-factor authentication (MFA). Passwords can be subjected to numerous cyber-attacks, including brute force. MFA provides

an additional layer of security and protects systems should passwords become known by unauthorized users.
- Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

Will inventory lists now be required for Low Impact sites? Based on the current requirements, is it safe to assume that cloud electronic access controls are acceptable for vendor remote access into low impact sites?

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Taunton Municipal Lighting Plant - 1

Answer	
Document Name	

Comment

The most concerning to us is Attachment 1, Section 6.3 in which the term "detecting" known or suspected malicious communications for vendors is

used. The term "detecting" is unclear to us. We are unsure if this would require continuous monitoring of the vendor's session, or if it is simply intended to at least manually review the vendor's session after the fact. Is the intent to provide constant real-time monitoring, which would be costly and time consuming?	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
With the consideration of the FERC NOPR. Additional architecture diagrams should be illustrated for a possible IDS/IPS implementation similar to when EAC under section 3 there were guidance architecture diagrams.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	
Document Name	
Comment	
In the Technical Rational, first sentence in the foreward, consider using language consistent with Section 6. Change ‘electronic remote vendor access’ to ‘electronic vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

No comment

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	
Document Name	

Comment

The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2020-03 Supply Chain Low Impact Revisions (Draft 2)
Comment Period Start Date:	2/25/2022
Comment Period End Date:	4/15/2022
Associated Ballot:	2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 2 ST

There were 75 sets of responses, including comments from approximately 167 different people from approximately 114 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. Do you agree the updated language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process,

Questions

procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

8. Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Santee Cooper	Chris Wagner	1		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					LaChelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Paul Camilletti	Santee Cooper	1,3,5,6	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Jennifer Bray	Arizona Electric Power	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Fred Meyer	Algonquin Power Co.	3	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
LaKenya VanNorman	LaKenya VanNorman		SERC	Florida Municipal Power Agency (FMPA)	Chris Gowder	Florida Municipal Power Agency	5	SERC
					Dan O'Hagan	Florida Municipal Power Agency	4	SERC
					Carl Turner	Florida Municipal Power Agency	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Richard Montgomery	Florida Municipal Power Agency	6	SERC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Company		
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State	7	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Reliability Council		
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State	10	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Reliability Council		
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion	6	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Resources, Inc.		
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Portland General Electric Co.	Ryan Olson	5		PGE Group 2	Brooke Jockin	Portland General Electric Co.	1	WECC
					Dan Zollner	Portland General Electric Co.	3	WECC
					Daniel Mason	Portland General Electric Co.	6	WECC
					Ryan Olson	Portland General Electric Co.	5	WECC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion	5	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Resources, Inc.		
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC Entity Monitoring	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. *Do you agree the updated language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.*

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends the SDT align the CIP-003 Attachment 1 Section 6 language with CIP-005-6 R2 and use NERC-defined terms where possible. The content of Section 6 should be included within Attachment 1 Section 3 and not made into a new section. Reclamation recommends adding "if technically feasible" to Section 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

Reclamation recommends the following changes to Section 6:

From:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

To:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including **Interactive Remote Access** and system-to-system **remote** access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for **identifying active** vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling **active** vendor remote access.

The phrase "determining active vendor remote access sessions" is not clear. Reclamation recommends using the same language as in the Technical Rationale, which refers more specifically to "when sessions are initiated."

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT considered your recommendations and concerns to better clarify the standard language.

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

As with the previous draft, Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS. Section 6.3 would require detection of malicious inbound and outbound communications for low impact BCS with vendor remote connectivity. In the current version and next effective version of CIP-005, Part 1.5 requires detection of malicious inbound and outbound communications only for medium impact BCS at **Control Centers**.

The Technical Rationale points out that Mediums already have other requirements ("use of intermediate systems and multi-factor authentication") which can be used to PROTECT against malicious communication; however, none of those requirements specifically

require that entities DETECT malicious communication at Mediums. Until this gap is fixed, entities will be expected to detect malicious communications at certain of their Low assets but none of their Medium assets outside of a control center.

In addition, BPA is concerned that by not properly limiting the scope statement for Section 6 to sites with vendor remote access, we may have to prove a negative.

BPA recommends the following ***revision***:

Section 6. Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) ***with vendor remote access*** identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include…

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The drafting team has reviewed your recommendations to improve the scope, and your concerns regarding the possibility of having to prove a negative to an enforcement entity. The SDT also recognizes your concerns that the detection of malicious communications is not required for Medium impact system, and has made some clarifying changes.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The introduction of "detecting known or suspected malicious communications" for low impact BES Cyber Systems would be more stringent as compared to CIP-005 R1.5 since Medium Impact BES Cyber Systems are not applicable in the current version of the standards without adding any additional reliability benefits.

Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The drafting team recognizes your concerns that the detection of malicious communications is not required for Medium impact system and addressed this in the Technical Rationale (TR).	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team addressed these concerns within the TR.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. See our response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy feels Attachment 1 Section 6.3 is not clear in its intention of the standard and obligation of industry. We feel Attachment 1 Section 6.3 needs to be drafted to be as clear as 6.1 and 6.2	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has further clarified the intent of Attachment 1 Section 6.3. Please see additional information in the TR.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
PNM supports the EEI inclusion of the word “active” in 6.1 and 6.2. However, with the inclusion of the word “active”, the current proposed language in 6.1 and 6.2 which reads, “where such access has been established under Section 3” may be redundant. PNM supports EEI comments regarding 6.3 to more specifically narrow the scope of detecting known or suspected malicious communications for both inbound and outbound “electronic vendor remote access, where such access has been established under section 3.”	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
patricia ireland - DTE Energy - 4	
Answer	No
Document Name	
Comment	
Refer to NAGF comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to NAGF.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. See our responses to each of your individual comments.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

BC Hydro appreciates the opportunity to reeview and provides the following comments.

BC Hydro's assessment is that the language proposed in CIP-003-X attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- The language used in CIP-003-X attachment 1 Section 6.3 is referring to 'known or suspected malicious communications'. BC Hydro recommends adding more clarity and provide examples of use cases and applicability. Specifically, context and usage of the term 'malicious communication' needs more clarity and BC Hydro requests to provide the context and usage with pertinent examples and use case scenarios to improve understanding and to better scope the requirements.
- Similarly, BC Hydro proposes defining and adding the term 'Electronic Vendor Remote Access' to NERC Glossary of Terms

- Bc Hydro also suggests that who and what is to be considered a 'Vendor' needs to be defined in the Glossary of Terms for clarity.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote access; however, this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.3 completely.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The team has added clarifying information in the TR.

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

For this question we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT added clarifying changes to both the language and the TR.

Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1

Answer	No
Document Name	

Comment

NextEra Energy respectfully submits the following language changes to Attachment 1 and Attachment 2 replacing "electronic vendor remote access" with "Vendor Electronic Remote Access" for consistency and clarification.

Consider the following language:

x Attachment 1

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with **vendor electronic remote access**. These processes shall include:

6.1 One or more method(s) for determining **vendor electronic remote access** where such access has been established under Section 3;

6.2 One or more method(s) for disabling **vendor electronic remote access** where such access has been established under Section 3; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications **supporting vendor electronic remote access**.

CIP-003-x Attachment 2

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 to mitigate risks associated with **vendor electronic remote access** may include, but are not limited to:

1. For Section 6.1, documentation showing **method(s) for determining vendor electronic remote access where such access has been established under Section 3 that may including the following:**

- steps to preauthorize access;
- alerts generated by vendor log on;
- session monitoring;

- Security Information Management logging alerts;
- time-of-need session initiation;
- session recording;
- system logs; or
- other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing **method(s) for disabling vendor electronic remote access where such access has been established under Section 3 that may including the following**:

- disabling **vendor electronic remote access** user or system accounts;
- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active **vendor electronic remote access;**
- disabling communications protocols (such as IP) used for systems which establish and/or maintain active **vendor electronic remote access**;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active v**endor electronic remote access**; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of **method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor electronic access communications that may including the following**:

- Firewall policies;

- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts;
- manual log reviews; or
- other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The drafting team has addressed these concerns in the current draft.

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	No
Document Name	

Comment

Anything prompting action at the low impact level must be very succinct otherwise risk overwhelming already taxed resources devoted to cyber security. More detail must be developed to limit the scope of communications that will be covered.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT is carefully balancing your concerns with the need to address identified cyber risks to the Bulk Electric System.

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No

Document Name	
Comment	
LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachement 1 Section 6 more closely resemble the language as written in the NERC Board resolution and the CIP-005 Standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team continues to try and improve the language using CIP-005 language as a reference point, however not all entities agree that CIP-005 language usage is more clear.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF previously recommended that the SDT align the language to include the word "active", which is utilized in both the Board Resolution and CIP-005 R2.4. The NAGF is concerned that using the word "electronic" may cause a differing definition and expectation to be developed over time compared to the objective of the language in the Board Resolution. Does the SDT view "active" and "electronic" as synonymous terms? If the SDT does not see "active" and "electronic" remote vendor access as synonymous further definition of "electronic" is required.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The drafting team does not see the terms “active” and “electronic” as synonymous. There were many comments asking for clarity of the term “active” in the last posting, some feeling that it was not limited to remote electronic communications. The SDT made clarifying changes to both the standard language and the TR.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA believes the proposed language is improved upon since the last posting; however, LCRA believes it would be more clear and consistent to have the language in Attachement 1 Section 6 more closely resemble the language as written in the NERC Board re solution and the CIP-005 Standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team does not see the terms “active” and “electronic” as synonymous. There were many comments asking for clarity of the term “active” in the last posting, some feeling that it was not limited to remote electronic communications. The SDT made clarifying changes to both the standard language and the TR.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI recognizes that the proposed changes under this project are intended to align with the NERC Board resolution, however, EEI is concerned that the proposed Draft 2 language in Attachment 1, Section 6 goes beyond the intent of the Board resolution by bei ng overly broad. In addition, the proposed language in Section 6 is not risk-based and could be understood to mean all low impact BES Cyber System communications are included. As a result, entities would be faced with difficult choices that include how to safely allocate scarce	

resources (i.e., limited budgets and qualified SMEs) to meet existing CIP-003 requirements while also covering the unfettered expansion of low impact BES Cyber System communications. To address this concern, we ask that the SDT employ a risk-based approach that allows entities to develop processes that focus their resources on those systems that represent known risks.

In addition to the above concern, EEI supports the proposed language in Section 6, subparts 6.1 and 6.2 but suggests some min or edits as indicated in the bold text below. In particular the proposed language for subpart 6.3 is not sufficiently aligned with communications as established under Section 3. The introduction of the new undefined term "vendor communications" needs additional explanation or clarification because it is treated separately and not aligned with Section 3. For these reasons, we recommend adding the text in bold to define the scope more clearly.

Section 6: Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible entity shall implement a process to mitigate risks associated with electronic vendor remote access. These process shall include:

6.1: One or more method(s) for determining **when active** electronic vendor remote access **has been initiated**; where such access has been established under Section 3;

6.2: One or more method(s) for disabling **active** electronic vendor remote access **when necessary;** where such access has been established under Section 3; and

6.3: One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound **electronic** vendor **remote access, where such access has been established under Section 3**.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has addressed these concerns in the current draft.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment
Based on the comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT believes we have met the requirements of the current SAR.

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
The language used in of the NERC Board resolution states the CIP-003 is "to include policies for low impact BES Cyber Sytems…". We agree with the SDT's interpretation that 3 controls listed in the resolution should be addressed not only in the CIP-003 R1.2, policies but in the plans required in CIP-003 R2 and Attachment 1. While the R2 additions are an expansion beyond the NERC Board resolution, they are required to meet the intent of the resolution. Because CIP-003 Attachment 1 is written to apply at the "assets containing low impact BES Cyber Systems" and not to just the "BES Cyber Systems", the 3 controls listed in the NERC Board resolution could be required to be applied to more than low impact BCS. This expansion in scope beyond low impact BCS is not required by the NERC Board resolution. The expansion could include additional controls being required for medium and high impact Cyber Assets beyond what are included in as "Applicable Systems" in CIP-005 R1.5 and R3. Regarding the control concerning malicious communication, we feel that this should be limited to only low impact BCS at Control Centers to align with CIP-005 R1.5. An interpretation of what the SDT has proposed could require the detection of malicious voice communication, text messages, or emails from anyone to anyone that is at an asset containing low impact BES Cyber Systems.

The NERC Board resolution includes the implementation of controls to "disable active vendor remote access." CIP-005 R2.5 addresses disabling active vendor remote access and R3.2 addresses terminating vendor initiated remote connections. The actions listed in Attachment 2 and the language used in the Technical Rational for Attachment 1 Section 6 Part 6.2 combine disabling and terminating as part of the required control. The SDT should limit the scope to disabling active vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. The SDT updated language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6 to better define the communication s scope. The SDT updated the TR to use the term "disable" instead of "terminate" to be consistent with the draft standard language.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term "vendor communications" needs explanation.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term "vendor communications" has been removed from the draft standard.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon believe registered entities could accomplish this, however it would be difficult to tell what the malicious intent really is. We do understand, however IDS can help with the inspection of packets. But without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term "vendor communications" needs explanation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term "vendor communications" has been removed from the draft standard.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question.	

Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term "vendor communications" needs explanation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term "vendor communications" has been removed from the draft standard.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Entities could accomplish this, however it could be difficult to tell what malicious intent really is. We do understand IDS can help with the inspection of packets. Without the information it could be expensive. Deploying controls at lows without having all of the information accounted for is concerning. This would require the need to have IPS on all of the low firewalls, including monitoring. Exelon has concerns around subpart 6.3 additional clarity is needed. The new term "vendor communications" needs explanation.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Additionally, the term "vendor communications" has been removed from the draft standard.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electrical Institute's (EEI) comments and believes the drafted language more adequately addresses the purpose/goal as stated in the SAR and Technical Rationale	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	No
Document Name	
Comment	
FMPA supports comments from Utility Services, Inc.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see our response to Utility Services, Inc.	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
Portland General Electric Company (PGE) supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI comments.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	No
Document Name	
Comment	
NST notes that the NERC BoT's resolution, as written, does not explicitly limit the application of a malicious code detection requirement to remote connections to or from vendors.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations about this topic with NERC compliance and legal staff. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No

Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
While we agree with the updated language as a whole, we support EEI's proposed modification to Attachment 1 Section 6, as it adds clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word “vendor”, not a NERC defined term, to the requirement from the previously posted : “One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications” doesn’t materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don’t feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn’t for a vendor would be overly burdensome.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.

Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	

Comment
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments below: ACES Comments: While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word "vendor", not a NERC defined term, to the requirement from the previously posted : "One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications" doesn't materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don't feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn't for a vendor would be overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment	
The MRO NERC Standards Review Forum (NSRF) agrees proposed language addresses the risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

We agee because this gives the ability to disconnect, we ask the drafting team to include examples of evidence for this requi rement (log ins?).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT provided examples of evidence for Section 6 in Attachment 2.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
It does address the risk, but as written increases some security requirements beyond what is required for Medium Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums has been discussed in the TR.	
Brian Lindsey - Entergy - 1	
Answer	Yes
Document Name	
Comment	

No Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While the proposed language addresses the risks outlined by the NERC Board resolution, adding the word "vendor", not a NERC defined term, to the requirement from the previously posted : "One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications" doesn't materially change this requirement is more stringent than those required by CIP-005 R1.5 for medium impact BES Cyber Systems NOT at Control Centers. Further reducing the scope of the requirement to only vendor communications, we don't feel reduces risks to an acceptable level for NERC or FERC. If entities are going to be required to detect malicious communications, it should be all or nothing. Additionally, vendor is not a NERC defined term, so having to prove each monitored communication path is or isn't for a vendor would be overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form.docx
Comment	

While GSOC agrees that the proposed language addresses the risks identified by the NERC Board Resolution, it is concerned that the absence of the term "active" broadens this requirement beyond the obligations set forth to manage vendor access for medium and high impact BES cyber assets. In particular, the language of the similar requirements for vendor access management in CIP-005-7, R2.4 and R2.5 focuses the requirements on determining and disabling "active vendor remote access sessions." The language proposed in Attachment 1, Sections 6.1 and 6.2, however, could be interpreted to apply to any authorized vendor remote access – regardless of whether or not the vendor has initiated or is in an active remote access session.

Such a requirement would result in low impact BES cyber assets being subject to more stringent security controls than high or medium impact BES cyber assets and appears to conflict with the Technical Rationale for these sections as provided on page 5 of the proposed Technical Rationale document. To ensure that the security controls applied to low impact BES cyber assets are commensurate with risk and not more stringent than those applied to high and medium impact BES cyber assets, GSOC recommends that the SDT mirror the language provided in CIP-005-7, R2.4 and R2.5 to the extent possible. For example, revisions could be made as follows:

For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access. These processes shall include:

6.1 One or more method(s) for determining active electronic vendor remote access sessions where such access has been established under Section 3;

6.2 One or more method(s) for disabling active electronic vendor remote access where such access has been established under Section 3

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT discussed the addition of the term "active" in section 6. The team decided that stating "as established under Section 3.1" meets the objective of the Board resolution. The SDT is attempting to make the language risk-based and

believes it is currently drafted to allow entities to draft their program in a way that meets their unique set up in regards to vendor remote access. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas Re appreciates the SDT and NERC legal looking into the issue of whether or not Part 1 of the NERC resolution has been satisfied. Texas RE suggests the SAR and the report do provide flexibility for the SDT to consider language for detecting known or suspected malicious communications for all inbound and outbound communications, and not be limited to vendor inbound and outb ound communications. Texas RE continues to recommend the SDT clarify that CIP-003 low impact monitoring obligations extend to all inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of vendor remote access. Texas RE notes this approach is consistent with FERC's January 20, 2022 Notice of Proposed Rulemaking (NOPR) regarding internal network security monitoring.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had several conversations with NERC compliance and legal staff about this topic. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations", were focused only on supply chain risks posed through vendor electronic access. Also see the draft TR for a discussion on vendor.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	

Xcel Energy agrees that Attachment 1 Section 6 addresses the risk malicious communication posed by vendors accessing low impact BES cyber systems from remote locations. However, there is a lack of clarity of which types of cyber assets are in scope for subp art 6.3. Xcel Energy suggests that language of "as established in section 3" be added to section 6.3 as it is in sections 6.1 and 6.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement “as established under Section 3.1” applies to all parts of Section 6.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

2. The standard drafting team (SDT) believes that remote access is a widely used and understood term. The team has added clarifying language to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to Utility Services, Inc.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Header 6.1 and 6.2 - Add the word “active” in the requirement and move “electronic” adjective. One or more method(s) for determining *active* vendor *electronic* remote access where such access has been established in Section 3.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT made clarifying changes to the current draft.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to EEI.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST suggests dropping "electronic" from the phrase, "electronic vendor remote access." The only kind of remote access to electronic devices (including Cyber Assets) that presently exists is electronic. In addition, NST believes the remote access terms the SDT has used in CIP-003 Sections 6.1, 6.2 and elsewhere should be consistent with the language in CIP-005, which addresses "vendor remote access," not "electronic vendor remote access." Consistent use of terms enables Responsible Entities with assets other than low impact to develop and apply controls across assets of differing impact levels.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. We understand the premise you are stipulating, however we have had comments as to whether remote access might also include the insertion of a thumb drive and dial up access into a system. The SDT made clarifying changes to both the standard language and the TR. The SDT added the word "electronic" to ensure that dial up connectivity or other non-electronic access, which could be considered remote by some, was not included in the requirements of this standard. Additionally, we have received comments regarding the use of the same terms as those in CIP-005, because it is believed the definition of the term used in CIP-005 is broader than the intent of the SAR and NERC in requiring the development of this standard.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to Utility Services, Inc.	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	

Dislikes 0	
Response	
Thank you, please see our response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electric Institute's (EEI) comments. Draft 1 of Attachment 1 Section 6 included the clarifying language "(including interactive and system-to-system access)" which was removed from Draft 2, making it unclear what forms of access are in scope. Additionally, the term "vendor" is an undefined term and should be clarified in the NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to EEI.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelon doesn't agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	

Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to Exelon.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelon doesn't agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to Exelon.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has provided more information on "remote" in the TR.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon does not agree that it's necessarily clear so can't agree that its widely understood. The term 'Remote' can mean different things…a vendor thats internal/on site, physically remote externally to the site versus remote to the company, or a Verizon wireless card… or is it up to the Registered Entity to define it?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has provided more information on "remote" in the TR.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

The SDT has used the word "electronic vendor remote access" and not the term "active vendor remote access" that is used in CIP-005-7 and in the NERC Board resolution. It is unclear why this inconsistency is needed or what the difference is between the two terms.

Furthermore when reviewing the Technical Rationale behind these proposed modifications, a footnote which had previously referenced guidance on the term "vendor" and how it may be used in the current version of CIP-013 and the future versions of CIP-005, CIP-010, and CIP-013, had been removed making for more confusion on what a vendor may be in this scope. Can the SDT please provide the reasoning for removing the footnote/reference from the Technical Rationale?

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT made these changes based on comments from a previous ballot and comment period.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Recommend using the CIP terms "interactive remote access" and "system-to-system access" instead of introducing a new term "Electronic vendor remote access." Also, CIP-005 uses "vendor remote access." Remote access implies "electronic" so "electronic" does not need inclusion in the term.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT previously received comments regarding the use of the terms included in CIP-005, because they are defined in a manner which may broaden the scope of the language drafted for CIP-003. The SDT made clarifying changes to the standard as well as the TR.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has provided more information on “remote” in the TR.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
More work should be undertaken to clearly define the terms remote access and the scenarios.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has provided more information on “remote” in the TR.	
Brian Lindsey - Entergy - 1	
Answer	No

Document Name	
Comment	
Generally "interactive" remote access is also used. Interactive means not only read only or view only access. This should be a part of the standard as if I am only viewing or retrieving read only data there is no ability for the remote connection to make changes or perform actions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has provided more information on "remote" in the TR.	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	
Please see NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to NEE, question 1.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	

Comment	
Recommend using the CIP terms of “interactive remote access” and “system-to-system access” instead of introducing a new term “Electronic vendor remote access.” Also, CIP-005 uses “vendor remote access.” Remote access implies “electronic” so “electronic” does not need inclusion in the term.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The term “interactive remote access” was removed due to comments received during a previous posting. The SDT added the word “electronic” to ensure that dial up connectivity was not included in the requirements of this standard.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As mentioned in comments related to Question 1 above, ' Electronic Vendor Remote Access' needs additional clarity to ensure proper understanding of applicability as well as the use of term 'Vendor' e.g., whether consultant using same infrastructure is considered vendor?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT added the word “electronic” to ensure that dial up connectivity was not included in the requirements of this standard. Also see the draft TR for a discussion on vendor.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	

Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Recommend using the CIP terms of "interactive remote access" and "system-to-system access" instead of introducing a new term "Electronic vendor remote access." Also, CIP-005 uses "vendor remote access." Remote access implies "electronic" so "electronic" does not need inclusion in the term.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The decision to remove the terms "interactive remote access" and "system to system remote access" was based on comments to a previous posting of this standard. The SDT added the word "electronic" to ensure that dial-up connectivity and/or use of removable media was not included in the requirements of this standard.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	

Answer	No
Document Name	
Comment	
PNM supports EEI comments regarding the needed clarity around “remote access” referring to user remote access, machine remote access, or both.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy agrees with EEI’s comments: “While the term “remote access” is generally understood, it is unclear what it means in the context of this Reliability Standard. Specifically, it is unclear whether the SDT meant this to mean user remote access, machine remote access or both. For this reason, we ask that the SDT provide clearer direction within the Technical Rationale.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	

Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP would like to see “Electronic Vendor Remote Access” as a clearly defined term. For example, is web-conferencing considered electronic vendor remote access?	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The drafting team has provided more information on “remote” in the TR.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	

Comment	
Recommend using the CIP terms of "interactive remote access" and "system-to-system access" instead of introducing a new term "Electronic vendor remote access."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT removed the terms "interactive remote access" and "system to system remote access" based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR for this update.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric (SIGE) does not believe that this language is clear or widely used. The most widely used description of remote access is interactive remote access. If the SDT intends to include system-to-system access then that should be made clear. Remote access should be clearly defined as interactive access and system-to-system remote access. SIGE proposes re-installing the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, "(including interactive and system-to-system access) to low impact BES Cyber Systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT removed the terms "interactive remote access" and "system to system remote access" based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR.	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Remote access should be clearly defined as including interactive and system-to-system remote access. CenterPoint Energy Houston Electric (CEHE) proposes re-instating the wording from Draft 1 Attachment 1 Section 6 to give additional detail to remote access, "(including interactive and system-to-system access) to low impact BES Cyber Systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT removed the terms "interactive remote access" and "system to system remote access" based on feedback from a previous comment period for this standard over concerns that those terms expanded the scope of the SAR.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
If "remote access" is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the "Interactive Remote Access" definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT received contrary responses with the belief that using the term "Interactive Remote Access" expands the scope of the SAR because of its formal definition in the NERC Glossary of Terms.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends adding "Vendor" to the NERC Glossary of Terms and proposes the following definition: Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts to supply equipment for BES Cyber Systems and related services. Vendor does not include other NERC-registered entities that provide reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). Vendor may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT addressed the term "vendor" in the TR.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
If "remote access" is going to be brought into scope for low impact sites and the intent is for it to be limited strictly to remote access conducted by vendors, then the term needs to be in alignment with the "Interactive Remote Access" definition. The manner in which Section 6 is currently written seems to imply that system-to-system communications will be included.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT received contrary responses with the belief that using the term "Interactive Remote Access" expands the scope of the SAR because of its formal definition in the NERC Glossary of Terms.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC agrees that remote access is a widely used and understood term and would suggest that the language used in Attachment 1 more closely mirror the language utilized in CIP-005-7 to reduce the potential for additional confusion, ambiguity, and subjective interpretation. Please see comments provided in response to question 1 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See our response to question 1.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	

Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see our response to MRO NSRF.	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes that the term "remote access" is commonly used to address electronic access originating from locations outside of protections established in an entities PSP and ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
The language is more clear, but does not really limit the effort to implement the control.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

We believe that the language is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

3. *Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification*.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Comments: Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a "remote location".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT realized that IRA across an ESP is the requirement for both High and Med, however, since neither of those definitions apply to Lows, the team included the language "as established within Attachment 1 Section 3.1". Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes "remote access" is any access that crosses this boundary.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the language "as established within Attachment 1 Section 3.1". Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes "remote access" is any access that crosses this boundary. If a vendor is "onsite" but starts the connection process outside this boundary, this connection should be considered remote access.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
Remote access, as widely understood today with regards to the CIP standards, involves interactive electronic access across an Electronic Security Perimeter. Low impact sites do not have an associated requirement for an Electronic Security Perimeter, so there is no reference point for what is considered a "remote location".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT realized that IRA across an ESP is the requirement for both High and Med, however, since neither of those definitions apply to Lows, the SDT included the language "as established within Attachment 1 Section 3.1". Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset	

containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes "remote access" is any access that crosses this boundary.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. The Cyber Assets identified as medium impact would not be applicable to Section 6.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT believes that the changes made to add this requirement have not impacted the way that mixed environments are currently being addressed. The Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro suggests that the use of word "Remote" will need clarification and perhaps a definition in the Glossary of Terms. For example, in the scenarios below, how will the "Remote" term be used? 1. On site, but electronically remote (i.e. has to go through EAP despite being at the station). 2. A "vendor" at the work location of Responsible Entity, also electronically remote (i.e. going through EAP). 3. "Traditionally" remote, off site, and electronically remote (also going through EAP).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT included the language “as established within Attachment 1 Section 3.1”. Section 3 for Lows is the requirement to create a network boundary for access to the low impact BES Cyber Systems from Cyber Assets outside the asset containing low impact BES Cyber Systems. Since this requirement has been in place for some time, the SDT believes “remote access” is any access that crosses this boundary.	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	

Please see NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to question 1.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF membership is concerned with the "remote locations" language in this question. Remote location is not used to describe the vendor's access in any version of the standard language. Is the SDT referencing geographic location or network topology? The standard language references inbound and outbound communications between the BES Cyber System and "Cyber Asset(s) outside the asset" (Section 3.1.i).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The concept presented by the SDT is that "remote" is based on the criteria established with Attachment 1, Section 3.1.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. The Cyber Assets that are identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We disagree that the intent of the NERC Board resolution is to address vendor access to low impact assets. Our understanding of the NERC Board resolution is that the controls are to apply to low impact BES Cyber Systems at assets that have low impact BES Cyber Systems. The SDT's interpretation could require the 3 controls to be applied to vendor remote access and communication to more than not just low impact BCS.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. While we agree the resolution is focused on the risk of vendor remote access to low impact BES cyber systems, the SDT believes the draft language is consistent with other sections of Attachment 1.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon ultimately believes this would require us to have an inventory list of the lows impact assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team believes the drafted language requires no more than what is required today to meet the other sections of Attachment 1.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon believe that ultimately, this would require us to have an inventory list of the lows impact assets.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The team believes the drafted language requires no more than what is required today to meet the other sections of Attachment 1.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
The new undefined term "vendor communications" needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using "active" electronic vendor remote access and in 6.3 add "…where such access has been established under section 3"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT added language about "access being established under Section 3.1" to the parent so it applies to the subparts of Section 6.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
The new undefined term "vendor communications" needs additional explanation. Recommend adding text in bold for clarity. In sections 6.1-6.3 the SDT should consider using "active" electronic vendor remote access and in 6.3 add "…where such access has been established under section 3"	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT added language about "access being established under Section 3.1" to the parent so it applies to the subparts of Section 6.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
"Vendor communications" is a new term. It doesn't scope this new term to communications "as established in Section 3" as the others do. "Vendor communications" is too broad of a term and wide open to many interpretations of the definition meaning.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT adjusted the language to help better clarify this term.	

Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes, the SDT has clarified the scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy belives the scope is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Brian Lindsey - Entergy - 1	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees in part that the language in Attachment 1, Section 6 is clear but offers some suggested edits for SDT consideration. (See our response to Question 1)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to question 1.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	

Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Although NST agrees Section 6 applies only to vendor remote access, it is our opinion that a malicious code detection requirement should not be limited to only vendor remote connections.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The NERC Board Resolution, and the subsequent approved SAR, focused the drafting team's work on vendor communications. It is outside the scope of the SAR to expand on that at this time.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	Yes
Document Name	

Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
Vendor remote access needs to be clear to convey remote access only	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made updates to the draft standard to clarify.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
6.3 language needs to be clearer and have a tighter bounded scoping to avoid the widest possible interpretation at audit. You can't go to Section 3 Electronic Access Controls evidence and show you are detecting things on all identified LERC and fully prove 6.3 as it is currently written. The intent of 6.3 should be added as a requirement to Section 3.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT made modifications to the proposed language in Section 6.3 to more closely tie it to the scope of Sections 3.1.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	

Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelons interpretation of the proposed standard views that this opens up access to 'any' areas that has a low.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Exelon.	
Kimberly Turco - Constellation - 6	

Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Exelons interpretation of the proposed standard views that this opens up access to 'any' areas that has a low.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Exelon.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelons interpretation of the proposed standard views that this opens up access to 'any' areas that contain lows.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment	
Exelons interpretation of the proposed standard views that this opens up access to 'any' areas that has a low	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The proposed language in Section 6.3 could be interpreted to include communication to people and all Cyber Assets at an asset that contains low impact BCS. The controls for active vendor remote access could also be required to be applied to all Cyber Assets at the asset and not just those that are part of a low impact BCS. We would suggest appending a statement consistent with the other two subsections of Section 6, "where such access has been established under Section 3."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3" applies to all parts of Section 6.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI disagrees that the language in Attachment 1, Section 6 clearly limits the scope to low impact BES cyber systems. While we agree with the changes made to Section 6, subparts 6.1 and 6.2; the proposed language in subpart 6.3 is not sufficiently narrow. (See our response to question 1 above.)	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see our response to EEI, question 1.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA believes that the current wording makes it unclear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA believes that the current wording makes it clear that only low impact BCS is applicable. Additionally, it is unclear if controls have to be implemented at the asset level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	

Answer	No
Document Name	
Comment	
much more work is needed to sufficiently scope the low impact assets which will be considered in scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the edits made to Section 6 clarify which low impact BES Cyber assets are in scope.	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	
Clarity is needed for when low impacts systems exist in conjunction with medium impact systems located at Medium BES Assets/Facilities. I.E. situations where there is a medium impact BES Asset/Facility that also contains low impact systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No

Document Name	
Comment	
Please see NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to question 1.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.3 completely.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. Applying measures against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response to EEI comments.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact because Medium controls are at the system level while Low controls are at the asset level. Recommend including Low Impact BES Cyber Systems in the Requirement language to bound the sub-requirements. As written, the auditor may expand the scope to include assets that do not impact the BES.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT believes adding this requirement has not impacted the way that mixed environments are currently being addressed. Cyber Assets identified as medium impact would not be applicable to Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems. Further information can be found in CIP-003 TR section 3, reference model 7.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Section 6.3 should either reference Section 3.1 or somehow limit to only low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated language in Section 6 so that the statement "as established under Section 3" applies to all parts of Section 6.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy believes additional clarity could be established by adding verbiage to 6.3 that includes "as established in section 3"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	
Comment	
Request clarification on mixed sites. This update does not address locations with a mixture of Low and Medium Impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. If low impact assets are mixed with medium impact assets then lows need to be highwater marked as medium or treated as distinct and separate systems.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	No

Document Name	
Comment	
The inclusion of 'where such access has been established under Section 3' appears to bring into scope electronic vendor remote access to Cyber Assets that **are not** low impact BES Cyber Systems, but on the same network as a low impact BES Cyber System based on the language of Section 3.1 ii 'using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s).' This is due to the fact that CIP-003 uses 'asset containing' as a boundary. Please consider the following two options – **Option 1**: Scope Section 6 specifically to Section 3.1 i, which would more accurately scope to only low impact BES Cyber Systems. *Section 3.1 i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);* **Option 2**: Do not reference Section 3 or any part thereof, but include the following language in Attachment 1 Section 6 – *'between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).'* 6.1 One or more method(s) for determining electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); 6.2 One or more method(s) for disabling electronic vendor remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside asset containing low impact BES Cyber System(s); and 6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and out bound vendor communications between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
There is confusion with the language used in Section 6 as to whether it pertains to the assets containing the low impact BES Cyber Systems (which may contain out of scope cyber systems) or the low impact BES Cyber Systems themselves.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. CIP-003 R2 as currently enforceable is applicable only to low impact BES Cyber Systems.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
While AEP believes the proposed changes to the CIP-003 Standard are trending in the right direction overall, there was language struck through that we think adds clarity to the scope of the section. The aforementioned struck through language in Attachment 1 Section 6 is in bold below:	

Section 6: Electronic Vendor Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor remote access **(including interactive and system-to-system access) to low impact BES Cyber Systems that includes:** To provide a more clear understanding that the language in this section limits scope to low impact BES Cyber Systems, AEP recommends reinstating the language above that was struck from this revision.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. Additionally, the SDT determined the language previously struck was in error and it has been reinstated.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
The lack of specificity in the "access to low impact BES Cyber Systems" verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, "assets containing low impact BES Cyber System(s)" which does not limit the scope to only the "low impact BES Cyber Systems". If the intent is to limit the scope to "low impact BES Cyber Systems" and not the "assets containing low impact BES Cyber Systems", then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. Section 3.1 does limit scope to low impact BES Cyber Systems contained within the low impact asset.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Comments: The lack of specificity in the "access to low impact BES Cyber Systems" verbiage could imply that an Entity will be required to document all vendor remote access or system-to-system access to the asset. This would include BES Cyber Systems, balance of plant for non-BCSs, and corporate business networks. The language in Section 6 states, "assets containing low impact BES Cyber System(s)" which does not limit the scope to only the "low impact BES Cyber Systems". If the intent is to limit the scope to "low impact BES Cyber Systems" and not the "assets containing low impact BES Cyber Systems", then significant changes would be warranted for CIP-002/CIP-003 to ensure low impact BES Cyber Systems are identified and that an Electronic Security Perimeter is established.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. Section 3.1 does limit scope to low impact BES Cyber Systems contained within the low impact asset.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	

While NST agrees the Section 6 language limits the scope to low impact BCS, it is our opinion that it does not adequately define the types of in-scope vendor remote access. Do Sections 6.1 through 6.3 apply to vendor remote access via dial-up? Rather than simply use a blanket referral to Section 3 in Sections 6.1 and 6.2, Section 6 should refer to specific sub-parts of Section 3 (e.g., Section 3.1, Part i).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the language is properly scoped.	
Likes 0	
Dislikes 0	

Response	
Thanks for your support.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes, the SDT has made the scope clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

5. *Do the examples in Attachment 2 Section 6 support your understanding of what is required in Attachment 1 Section 6? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification*.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Comments: Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes implementation of the suggested methods can be applied at the system level and wouldn't require identification of individual Cyber Assets or Cyber Asset lists. The SDT does not believe the SAR allows this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s). Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No
Document Name	
Comment: Thank you	

The examples provided support what is required in Attachment 1 Section 6. Clarification in the language used is suggested, al ong with an additional example for vendor machine to machine remote access:

Electronic Vendor Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation **AND EVIDENCE OF IMPLEMENTATION** showing:

 DOCUMENTED steps to preauthorize access **ALONG WITH AUTHORIZATION RECORDS**

 CONFIGURATION OF alerts generated by vendor log on;

 PROCEDURES FOR THE USE OF VENDOR session monitoring **AND SESSION MONITORING LOGS**;

 Security Information Management logging alerts; **- REDUNDANT TO #1, CAN BE REMOVED**

 DOCUMENTED STEPS AND LOGS FOR time-of-need session initiation;

 DOCUMENTED STEPS AND LOGS FOR VENDOR REMOTE ACCESS session recording;

 DOCUMENTATION AND CONFIGURATION OF system logs **SHOWING VENDOR REMOTE ACCESS CONNECTIONS**

 DOCUMENTATION OF ELECTRONIC ACCESS CONTROL RULES PERMITTING INBOUND VENDOR MACHINE TO MACHINE COMMUNICATION; or

 other operational, procedural, or technical controls.

For Section 6.2, documentation showing **THE PROCESS FOR:**

 disabling vendor remote access user or system accounts;

 disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/ IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing active vendor remote access;

- disabling communications protocols (such as IP) used for systems which establish and/or maintain active vendor remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access; or
- other operational, procedural, or technical controls.

For Section 6.3, documentation showing implementation of:

- Firewall policies **IMPLEMENTING MALICIOUS TRAFFIC INSPECTION**;
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
- Virtual Private Network (VPN) hosts **IMPLEMENTING CONNECTION INSPECTION**;
- manual log reviews; or
- other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT included examples of evidence in Attachment 2.

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

Most of the suggested methods of achieving compliance go beyond the current requirements for low impact sites. Also, most of these methods require uniquely identified systems or assets, which is currently not required for low impact sites. If the intent of these

proposed methods is to create a set of requirements similar to those for Medium Impact BES Cyber Systems, then the recommendation would be to eliminate CIP-003, R2 and incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes implementation of the suggested methods can be applied at the system level and wouldn't require identification of individual Cyber Assets or Cyber Asset lists. The SDT does not believe the SAR allows for this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s). Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Not clear if VPN connections established with support vendors fully adheres to requirement or additional steps are required s uch as an IDS/IPS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. All connections established through Attachment 1 Section 3.1 are in scope for Section 6.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	No
Document Name	

Comment	
Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – "administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access." Attachment 1, Section 6 does not say "active vendor remote access." Next that bullet is inconsistent with the first Attachment, 6.2 bullet – "disabling vendor remote access user or system accounts."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – "administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access." Attachment 1, Section 6 does not say "active vendor remote access." Next that bullet is inconsistent with the first Attachment, 6.2 bullet – "disabling vendor remote access user or system accounts." Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – "Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access)."	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – "administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access." Attachment 1, Section 6 does not say "active vendor remote access." Next that bullet is inconsistent with the first Attachment, 6.2 bullet – "disabling vendor remote access user or system accounts."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	

Additional ephasis should be put on Programmatic non technical methods of allowance to clarify that processes can be leverage rather than purely technical methods.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Agree in principle with these examples Request the Measures (Attachment 2) use language consistent with the Requirements (Attachment 1). Attachment 2, 6.2 includes a bullet – "administrative control documentation listing the methods, steps, or systems used to disable active vendor remote access." Attachment 1, Section 6 does not say "active vendor remote access." Next, that bullet is inconsistent with the first Attachment, 6.2 bullet – "disabling vendor remote access user or system accounts." Request consistency or clarification between CIP-003 and CIP-005. CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 use different language than the proposed CIP-005, Part 2.5 Requirement – "Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access)."	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	

Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Firewall Policy and Virtual Private Networks aren't the greatest examples of capturing whats in Attachment 1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes

Document Name	
Comment	
Yes, the examples support our understanding of what is required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	

Attachment 2 Section 6 includes multiple uses of 'vendor remote access' and 'active vendor remote access.' To ensure a consistant scope to Section 6 consider changing all to '***electronic vendor remote access***.' disabling ***vendor remote access user*** or system accounts disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN,Remote Desktop, remote control, or other hardware or software used for providing ***active vendor remote access*** disabling communications protocols (such as IP) used for systems which establish and/or maintain ***active vendor remote access***; administrative control documentation listing the methods, steps, or systems used to disable ***active vendor remote access***;	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made clarifying changes to the draft language.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes that examples in Attachment 2 provide clarity to what is required in demonstrating compliance with Secti on 6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State mostly agrees however, the example of Steps to Preauthorize is confusing and too open-ended.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI, question 5.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF believes that the example are clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that Attachment 2, Section 6 examples support what is required under Attachment 1, Section 6.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC recommends that the language in Section 6.1 be revised to more closely mirror the language of CIP-005-7, R2.4, which would more clearly indicate the time frame and intent/activities to which the requirement and documentation should be focused.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The examples listed for Section 6.2 include controls for disabling and controls for terminating remote access. In addition, these examples use the terms “vendor remote access” and “active vendor remote access” but do not use the “electronic vendor remote access” term used in Attachment 1. While we do not think the term “electronic vendor remote access” should be used at all, there should be consistency throughout the document and preferably, consistency throughout the CIP Standards.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The SDT asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST has no comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes

Document Name	
Comment	
Thank you for your support.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes that a considerable amount of research would be needed before many respondents would be able to provide a well-informed answer to this question. We note the December 2019 "Supply Chain Risk Assessment" report states, "More than 99% of the responders (to a survey question about costs and benefits) agreed with the draft response that it was premature for CIP-013 registered entities to determine or estimate costs or benefits associated with the implementation of the standard…" That said, NST believes the cost to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3 and on the number of facilities where controls may need to be applied.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	

Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Until additional clarity is provided on the scope and intent of the proposed modifications, the overall cost is difficult to ascertain.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the proposed draft clarifies the scope and intent of the standard modifications.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Exelon.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Registered Entities could incur significant costs implementing considering the Low Cyber Asset inventory included.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Exelon.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes and configuration.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Registered Entities would incur significant costs implementing, considering the Low asset inventory included in the scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes and configuration.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The expansion of the requirement to detect suspicious malicious communication to systems that may not have routable communication and to systems that are not at a Control Center, as is required for high and medium impact, imposes costs that are not consistent with the risks as determined by previous Standard Drafting Teams. Furthermore we believe the SDT is only accounting for the cost of the equipment that would be responsible for performing the tasks of Section 6. While this is one cost to consider, there may be additional resources required to allow for implementation of such technology	

including but not limited to additional staffing, training, or other equipment that would allow a SIM/SEM/SIEM or IDS/IPS to have visibility.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6. Please see the TR for additional information. The SDT understands the cost of implementing a new requirement includes equipment as well as cost of training or staffing employees.	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	
Comment	
Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementin g this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal challenges to entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	

There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. This could pose fiscal challenges to entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
Any low impact related changes are likely to lead to significant scope creep and potentially many underlying, unknown costs that will be incurred.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	

The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The MRO NSRF has concerns about the potential of ineffective costs. Due to recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors the cost of implementation of the Requirements is at a much higher risk than what would normally be expected. Higher than expected costs may result in the need for a longer or adaptive implementation timeline.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes ,and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Although the cost may differ between entities, BC Hydro's assessment is that the impact may change based on understanding & clarity of terms and scope of application. As outlined in BC Hydro's comments to Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However, the requirement in CIP-003-X Section 6.3 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5, where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS out of scope.

Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Making this a requirement on all low impact BES Cyber Systems would be extremely expensive because new equipment must be installed at each low location to monitor for remote vendor access, allow for the ability to terminate sessions and detect malicious code. It would be more cost effective to create a risk-based approach that would target those low impact BES Cyber Systems that could have the most potential impact on the BES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

There are many entities that have a large amount of low impact sites that are in remote locations and struggle with limited bandwith that will be impacted. With the recent supply chain and staffing issues you will have higher than normal costs to implement these requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	

Xcel Energy is concerned with meeting the demands of section 6 in a cost effective manner at this time. World events have created issues with supply chain and receiving the needed products to perform activities required in the standard in a timely and cost effective manner. The vast number of low impact sites as compared to high and medium sites will cause a sudden surge in demand and cause prices to rise dramatically. The standard drafting team should take these issues into consideration in their implementation plan to spread costs and demand for products across and longer span of time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The SDT realizes there are unknowns with implementation and has increased the implementation plan to 36 months to account for this.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES comments: This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	

Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
This is very dependent on how an entity chose to implement it's low impact electronic access controls, the size of the organization, and if the organization has medium or high impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The changes limit the scope of what traffic must be monitored, but the technology and resources needed to conduct the monitoring remains the same.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	

Answer	No
Document Name	
Comment	
Depending on the solution(s) determined by NIPSCO, cost would most likely be a factor to purchase the equipment and resources necessary to achieve the goal of securing vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The scope should be narrowed to just where the risk exists as opposed to a broad swath of assets. The way it is written it implies that all communications need to be monitored to determine malicious communications through vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes the modifications have limited the scope of Section 6.	

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	No
Document Name	
Comment	
Due to supply chain issues and other geopolitical factors, it is difficult to determine the cost effectiveness of implementing this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003 Attachment 1 requirements and prove detrimental to a cost-efffective approach. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes that the modifications have limited the scope of Section 6.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends this project may be a good avenue to incorporate low impact requirements into these standards to avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT does not believe the SAR allows this team to incorporate low impact sites throughout the rest of the CIP standards, as appropriate, under the applicable systems column(s). Additionally, as currently structured, entities with low impact only are only subject to CIP-002 and CIP-003.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

Comments: These modifications, as they are currently written, could be misinterpreted, which would result in a significant expansion of scope of the CIP-003 Attachment 1 requirements and prove detrimental to a cost-efffective approach. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration. The team also believes the modifications have limited the scope of Section 6.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC is concerned that compliance with Section 6, as proposed, may require a significant investment of resources, specifically that such investment is beyond what is applied to protect high or medium impact BES cyber assets despite the fact that such investment may not yield commensurate reliability and security benefits.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications to Low Impact BCS and not all Mediums is addressed in the TR.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost-effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	
Document Name	
Comment	
We will need more information to adequately assess the cost-effectiveness of the proposed approach	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	

Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form_02252022 Presentation FINAL COMMENTS v2.docx
Comment	
To be "cost effective", this implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change. Additional staff and procedures will be required to monitor this level of detail to meet the requirements of CIP-003.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT is attempting to make the language risk-based and believes as it is currently drafted allows entities to draft their program in a way that meets their unique set up in regards to vendor remote access, timeframes, and configuration.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on the question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	
Document Name	
Comment	
SIGE will not provide a response to the cost effectiveness of the proposed changes to CIP-003-x.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
A longer implementation timeline would offer more cost effectiveness. This would allow industry to spread their investments and capital purchases.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT increased the implementation plan to 36 months based on industry feedback.	

7. The SDT is proposing an 18-month implementation plan for Attachment 1, Section 6.1 and 6.2. The proposed implementation time frame for Attachment 1, Section 6.3 is 24-months. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel/vendors appropriately.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	No
Document Name	
Comment	
BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for	

installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: "If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity." While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Sections 6.1 and 6.2 will not have equivalent language for Mediums without ERC until CIP-005-8 R2.4 and R2.5 are adopted. Therefore, BPA recommends that implementation of these sections should be aligned with the passage of CIP-005-8 to avoid entities having to monitor their Low assets but not their Mediums without ERC and/or Dialup. Section 6.3 has no current equivalent language in CIP-005-8 (nor any other standards) for Medium impact BES Cyber Systems except at Control Centers. Until then, entities will be expected to detect malicious communications at certain Low assets but none of their Medium assets outside of a control center. This is a significant gap; BPA recommends that the drafting team delay Section 6.3 until CIP-005 is expanded to include Mediums outside of Control Centers.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
After further consideration, we believe that a 36 month implementation timeline would be most appropriate for incorporating all the revisions in Project 2020-03. This will allow for proper installation, testing and documentation of new controls across a large inventory of sites and assets. This timeline would also be more feasible given the current supply chain challenges across industry.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The expansion of scope for vendor remote access monitoring and malicious communication monitoring may require new technology to be implemented within the program. The implementation for said technology for a large utility will require a longer implementation than 24 months.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
36 months minimum as additional staff or staff augmentation would have to be employed as there would be a significant amount of design, planning, testing, and finally, deployment of solutions to the affected assets in the field.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS feels that a 24-month implementation plan would be a reasonable timeframe to implement process, procedures or technology to meet the proposed language in Sections 6.1 and 6.2, in addition to Section 6.3. It may be necessary to design and implement multiple solutions to meet the proposed language in Section 6 across the various environments in which low impact assets are in use. Alternatively, a single solution which could be applied across a broader group of low assets may require significant design changes to process, procedures and/or technology.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Due to supply chain constraints on security equipment we believe an additional 12 months should be included or an exception were procurements happens within that time frame to adhere compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: "If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity." While this would need additional details developed, it would provide the industry with assurance	

that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. BHE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
A 24 month implementation is desirable due to budget, supply chain, and resources to implement solutions for SRP's Generation fleet.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	

Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Section 6.3, to allow entities more time to implement, the required control, if necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
AEPCO is signing on to ACES comments below. ACES comments: Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new technology implementation, there needs to be allowances at least for Attachment 1, Setion 6.3, to allow entities more time to implement, the required control, if necessary.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT has changed the implementation plan to 36 months.

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	

Comment
PNM supports EEI comments regarding the implementation timeframe for 6.3 to be extended to 36-months if the scope of 6.3 is not sufficiently narrowed as mentioned in the comments for question 1.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see our response to EEI.

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	
Comment	
Xcel Energy is concerned with meeting the implementation demands of section 6 within the proposed timeline identified in the implementation plan. World events have created issues with supply chain and obtaining the needed products and staff to perform activities required in the standard in a timely manner. The vast number of low impact sites as compared to high and medium si tes will cause a sudden surge in demand and cause prices to rise dramatically. Additionally, an industry-wide staffing shortage will slow efforts to implement and maintain newly procured products. The standard drafting team should take these issues into consideration in the ir implementation plan to spread costs and demand for products and staff across and longer span of time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
As mentioned in Question 6, many entities have large amount of low impact sites that are in remote locations and struggle with limited bandwith which makes procruement, and implementation of new hardware and software difficult. There is the other challenge of the recent supply chain and staffing issues that will also impact implementation timelines. The supply chain being taxed all at once by utilites to meet the short timeline should must be taken into consideration.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #7.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends a longer implementation plan, e.g. more than ~ 36 months considering the cost and scope impact as identified in comments to Questions 1 and 4 above. Once the clarity of terms and definitions is obtained as identified in comments to Questions 1 and 4, BC Hydro will be in a better position to provide an alternate detailed implmentation plan to meet the target completion deadline.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The MRO NSRF anticipates the procurement and implementation of new software, hardware, and associated services needed to detect vendor's malicious communications to be particularly challenging given recent supply chain issues, industry-wide staffing shortages, and other geopolitical factors. Registered Entities across North America will all be attempting to procure needed solutions in a relatively small window of time. This will create a deficit of supply with increased demand and will drive up costs. That, along with current staffing shortages and geopolitical events, may produce scenarios that will prevent a responsible entity from meeting the effective date set in the approved implementation plan. The MRO NSRF suggests the SDT align with NERC legal staff to allow for a provision in the imple mentation plan that would provide an opportunity for entities to request extensions based on the aforementioned factors.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to MRO NSRF.	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	No
Document Name	
Comment	

- NextEra Energy requests consideration of a 36-month implementation period due to a large number of sites (in the hundreds) requiring assessment and potentially new equipment and/or process implementation. The work must be planned and typically will be scheduled with planned maintenance and scheduled generation outages.
- The last few years the supply chain has adversely impacted maintenance including staffing and is expected to impact the implementation.

• Entities may need to evaluate and update vendor, supplier, customer and other agreements and contracts.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
Given the uncertainty regarding the exact scope of implementation across low impact and all vendor communications it is hard to believe the 18 months will be sufficient timing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Brian Lindsey - Entergy - 1	
Answer	No
Document Name	
Comment	
There could be additional needs for technology purposes which would create funding needs based on funding cycles and implementation. Strongly recommended to inceas all sections to a 24 mth implementation.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Again this is very dependent on the size of the entity, if the entity has medium or high impact BES Cyber Systems, if the entity has medium or high impact BES Cyber Systems at Control Centers, how many low impact BES Cyber Systems the entity has, and if supply chain will play a role in delaying the implementation of the controls for entities. Because of potential supply chain issues and new	

technology implementation, there needs to be allowances at least for Attachment 1, Setion 6.3, to allow entities more time to implement, the required control, if necessary.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
There is a high likelihood that new technology controls will be required to effectively meet the intent of these new requirements. Implementation of new technology takes time and careful consideration. Additionally, current supply chain challenges may pose an additional risk to effectively implementing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI appreciates the two-phase implementation plan for Attachment 1, Section 6 and supports the proposed 18-month implementation plan for subparts 6.1 and 6.2. However, we do not agree that an additional 6 months to complete subpart 6.3 is adequate, particularly given the current proposed language could be interpreted to mean all low impact BES Cyber System communication. Moreover, if the current language is not narrowed consistent with a risk-based approach it may be a significant challenge for some entities to complete this work in 36 months. EEI previously noted that there will be substantial work to complete 6.3 and companies are also facing significant supply chain issues/delays to secure materials necessary to implement these changes. For these reasons, the implementation plan should be at a minimum of 36 months.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	No
Document Name	

Comment
NVE expects implementation of Section 6.3 to require the purchase of a significant amount of new equipment. Hundreds of Registered Entities will all be purchasing intrusion detection systems at the same time, and within a short deliverable window to allow time for installation, resulting in even greater supply chain issues. Please consider adding something like the following to the implementation plan to address this potential issue: "If the Responsible Entity encounters significant supply chain issues, the Responsible Entity may request an extension from the Regional Entity." While this would need additional details developed, it would provide the industry with assurance that supply chain issues outside of their control would not result in non-compliance. An example of an extension might be equal to the time between placing orders for needed equipment and receiving said orders. NVE also requests NERC consider ways to work with equipment manufacturers to try to address the increased demand for this equipment.

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Given the potential impact of expanded scope of Section 6.3, GSOC would respectfully request a 24 month implementation period given the current state of global supply chain lead times.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire stand ard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. One collective implementation time frame. Because of the significant changes proposed by the SDT, can we set the entire standard to a 36 months implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Until additional clarification is provided on the scope and intent of the proposed changes, it's unclear if the drafted implementation timelines are sufficient to implement the requirements.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Clarifying changes have been made to the draft language and the implementation plan has been set to 36 months.	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by the Bonneville Power Administration (BPA).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to BPA.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes the time required to implement the proposed requirements could be significant, depending on how a given Responsible Entity has addressed Electronic Access Controls requirements in CIP-003-8, Attachment 1, Section 3 and on the number of facilities where controls may need to be applied. NST recommends a 24-month implementation time frame for all of Attachment 1, Section 6 requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	No
Document Name	
Comment	
PGE supports the survey response provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	No
Document Name	
Comment	
We would rather have one date of 24 months for the whole thing. Simpler to track and entities are going to need the time for various reasons. Some that don't have IDS capabilities at all their sites will have to order and receive and then implement a lot of equipment at a lot of sites. The 6.1 and 6.2 can be shorter for TO/TOPs that just have substations, or for those with only control centers. With the wide diversity of vendor situations out there on everything from a small solar to a string of wind turbines to a large Generation facility and all matters of variety of vendor arrangements and support, the timeframe and implementation plan is not simple. We do not want to make the assumption that 6.3 is 'hard' and needs more time and 6.1 and 6.2 are 'easier' and can be done quicker. In some cases, it might be the opposite. Whatever the maximum implementation time is, give that to everyone.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Comments: These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has made clarifying changes and set the implementation plan to 36 months.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
These timeframes are sufficient assuming that a significant expansion in scope isn't being proposed. Please reference previously provided comments for additional detail.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has made clarifying changes and set the implementation plan to 36 months.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

If all examples in Attachment 2 are ever required then we believe that additional time above the 18 months may be required.	
Likes 0	
Dislikes 0	
Response	
Thanks you for your comment. The SDT has changed the implementation plan to 36 months. The examples within Attachment 2 are just examples and is not a comprehensive list.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF has no comments.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Consider large-scale supply chain and implementation issues. If all entities request supplies at the same time, what will be the supply chain impact?	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has changed the implementation plan to 36 months.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The ability for entities to apply these control may be limited by the availability of equipment and the vendors qualified to install them. The SDT should request that NERC provide information on the expected number of substations that may be required to implement these controls. It may be necessary to include an automatic extension of the time allowed for implementation, if necessary, equipment and personnel to perform the installation are not available.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months based on industry feedback. The ERO Enterprise will address any industry-wide impacts as they arise.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Don Stahl, Black Hills Corporation, 3, 5, 1, 6; - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 6, 5, 3, 4; Richard Montgomery, Florida Municipal Power Agency, 6, 5, 3, 4; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on the question.	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
If scope of this standard is tightened to what FE believes is the spirit of the standard, we feel we could follow the propose d implementation plan. As it is written, we feel the vagueness of the draft leaves ambiguity and would require a longer implementation plan to fulfill our obligation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT changed the implementation plan to 36 months and updated the draft language with clarifying changes.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response

8. *Provide any additional comments on the standard and technical rationale document for the standard drafting team to consider, if desired*.
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	
Comment	
These 'low' requirements as written seem to be more stringent than what highs and mediums have to comply with today. Highs and Mediums have to determine 'active' sessions and have a method to disable remote access. That is far easier than determining what constitutes malicious inbound and outbound communications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Daniel Mason - Portland General Electric Co. - 6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes it is short-sighted to add a new requirement to CIP-003 for malicious communications detection that is limited to vendor remote access only. Advocates for this limitation seem to be ignoring the possibility a Responsible Entity's own remote computer systems could be compromised by attackers and used to deliver malware to BES Cyber Systems (BCS) at BES assets containing low impact BCS. In addition, NST believes that limiting the scope of monitoring and detecting to only vendor remote access either may not be practical or may result in sub-optimal designs that would need to be updated should monitoring and detecting requirements be expanded in the future. Given the likely time, effort, and expense associated with implementing a solution for malicious code detection (using IDS or similar technology), we think it only makes sense to require it for all remote access. NST also notes that in its recent NOPR proposing "Internal Network Security Monitoring" requirements for high and medium BES Cyber Systems, FERC indicated it is interested in the possibility of applying "INSM" requirements to low impact, as well. This suggests to us that while FERC might approve the current set of proposed supply chain revisions to CIP-003, were they to be approved by industry ballot and the NERC board, they might also direct NERC to further modify CIP-003 to apply malicious communications detection requirements to any remote access that uses routable protocols outside BES assets containing low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT had several conversations about this topic with NERC compliance and legal staff. Based on these discussions and a review of the Supply Chain report, the team determined that the SAR and the NERC Board: "Resolution for Agenda Item 8.d: Supply Chain Recommendations" were focused only on supply chain risks posed through vendor electronic access. The SDT believes the drafted standard meets the current objective from the NERC BOT and SAR. While looking “forward” to future requirements and/or	

potential standards that might be considered, it is beyond this teams current scope, which is focused solely on supply chain and vendor's access.	
Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to Utility Services, Inc.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See Comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Selene Willis - Edison International - Southern California Edison Company - 5	

Answer	
Document Name	
Comment	
See Comments submitted by the Edison Electric Institute." with your ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
SDT should consider defining the term "Electronic Vendor" in the NERC defined Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT modified the language to remove this term.	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	

SDT should consider defining the term "Electronic Vendor" in the NERC defined Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT modified the language to remove this term.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
What is meant by '**Electronic** Vendor'? Currently it's not a defined term, SDT should consider making this a NERC defined glossary term.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT modified the language to remove this term.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
What is meant by '**Electronic** Vendor'? Currently it's not a defined term, SDT should consider making this a NERC defined glossary term.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT modified the language to remove this term.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
All proposed controls should be limited to only low impact BES Cyber Systems as opposed to assets containing low impact BES Cyber Systems. The proposed control for detecting malicious communication should be limited to: 1. Only low impact BES Cyber Systems using a routable protocol to communicate across the asset boundary and, 2. Only Control Centers (to align with CIP-005-7 R1.5)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made changes to reduce the scope based on only those communications that are established through Attachment 1, Section 3.1. The SDT asserts that the SAR applies to all low impact facilities as identified in CIP-002.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	

For future reference, request redline to last approved since that shows the true SDT proposed updates. Recommend updating R1.2.6 by removing "Electronic" from "Electronic vendor remote access security controls." The security concern is vendor remote access. Recommend updating Attachment 1 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6 Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says "detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP." 6.3 says "detecting known or suspected malicious communications for both inbound and outbound vendor communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers. Recommend updating Attachment 2 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT made clarifying changes regarding the comment about "electronic vendor". Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	
Document Name	

Comment
No comment.

Likes 0	
Dislikes 0	

Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Dwanique Spiller	
Answer	
Document Name	
Comment	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. NVE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The TR has been updated.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
In the proposed Draft 2 of CIP-003-x, the undefined term "Electronic Vendor" has been used eleven times (including within Section 6 of Attachment 1). It is unclear what is meant by the use of this term and if this term is to remain within this Reliability Standard, the SDT should provide needed clarification through the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT has removed the term.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF membership recommends that the SDT consider providing reference architecture diagram(s) similar to previous reference model provided in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2016-02 team is preserving the reference documents that were in the GTB of CIP-003-8 in TR documents going forward. The diagrams that reference section 3 still apply to this draft of the standard and any communication crossing those boundaries are still appropriate.	

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Brian Lindsey - Entergy - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Mike ONeil - NextEra Energy - Florida Power and Light Co. - 1	
Answer	
Document Name	

Comment

- Please provide redline to last approved since that shows the true SDT proposed updates.
- Please apply NEE's response to question 1 respectfully submitting updated language CIP-003 Attachment 1, Section 6 and Attachment 2, Section 6 to the standard and technical rationale document.
- Page 4 " The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access," change to "**The SDT agreed to retain Section 3 and establish Section 6 to address low impact vendor electronic remote access,"**
- Page 5:
- "establish and disable electronic vendor remote access." to be "**establish and disable vendor electronic remote access."**
- "low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary." to be "low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active **vendor electronic remote access** sessions are initiated; and (3) disable active **vendor electronic remote access** when necessary."
- Attachment 1 Section 6 Part 6.1 – Determining V**endor Electronic Remote Access**
- "associated with malicious communications and electronic vendor remote access." to be **"associated with malicious communications and vendor electronic remote access."**
- Attachment 1 Section 6 Part 6.2 – Disabling **vendor electronic remote access**
- Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable electronic vendo r remote access." to be **"Enhanced visibility into vendor electronic remote access** and the ability to terminate **vendor electronic remote access** could mitigate such a vulnerability. The obligation in Section 6.2 requires that entities have a method to disable **vendor electronic remote access**.

- Page 6
- Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications for **vendor electronic remote access**

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The team made clarifying changes to the draft language of the standard and updated the TR.

George Brown - Acciona Energy North America - 5

Answer	
Document Name	

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this questi on.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response to MRO NSRF.

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

The MRO NSRF would like to thank the Standard Drafting Team, NERC Staff and all other contributors for their work on this project.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
For future reference, request redline to last approved since that shows the true SDT proposed updates. Recommend updating R1.2.6 by removing "Electronic" from "Electronic vendor remote access security controls." The security concern is vendor remote access. Recommend updating Attachment 1 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6 Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says "detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP." 6.3 says "detecting known or suspected malicious communications for both inbound and outbound vendor communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers. The low requirement may encompass email, phone, and or mail communications from vendors, because of the vague language used. Recommend updating Attachment 2 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SDT made updates to clarify the language in the standard. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	
Document Name	
Comment	
BC Hydro ackowledges the effort and hard work SDT put into putting these complex changes to CIP-003-X. As identified in comments to Questions 1 to 4 above. The definitions of terms and clarity of application with some specific industry use case examples will help providing a more clear understanding and likely result in a faster and appropriate approvals of these proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT reviewed Attachment 2 and made clarifying changes. The team asserts the examples of evidence listed in Attachment 2 is not a comprehensive list.	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates the comments from the Edison Electric Institute (EEI) for questions #8.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see our response to EEI.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
For future reference, request redline to last approved since that shows the true SDT proposed updates. Recommend updating R1.2.6 by removing "Electronic" from "Electronic vendor remote access security controls." The security con cern is vendor remote access. Recommend updating Attachment 1 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6 Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says "detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP." 6.3 says "detecting known or suspected malicious communications for both inb ound and outbound vendor communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers. Recommend updating Attachment 2 by removing "Electronic" from "Electronic vendor" for consistency with Requirement R1.2.6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made updates to clarify the language in the standard. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Alliant Energy appreciates the Standard Drafting Team's work on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy would like to thank the drafting team for their diligent work and bringing forward language to address the concerns identified by the NERC BOT.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
patricia ireland - DTE Energy - 4	
Answer	

Document Name	
Comment	
We remain concerned that the CIP-003 Attachment 1, Section 6.3 requirement for malicious communication places a heavier compliance burden on low impact assets than High and Medium, as deliniteated in CIP-005 (2.4 and 2.5). Simply extending the the implementation timeframe for this requirement does not address that basic inconsistency.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Applying measures to mitigate against malicious communications being applied to Low Impact BCS and not all Mediums is addressed in the TR.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Thank you to the SDT for their efforts and allowing AEPCO to participate in the drafting process.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	

Comment	
My intended vote for this ballot was negative based on the comments provided in this survey. However due to technical issues with the voting platform while casting my vote it is shown as affirmative. If possible please replace my affirmative vote with a negative vote.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Votes cannot be changed in the system. If you experience issues with the system in the future, please reach out 24-48 hours prior to the comment period/ballot close so we can look into it.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see our response to EEI.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	

We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE continues to have the following additional recommendations for the SDT: • Include language for (1) software integrity and authenticity, (2) information system planning and (3) vendor risk and procure ment controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010. • Include vendor multi-factor authentication (MFA). Passwords can be subjected to numerous cyber-attacks, including brute force. MFA provides an additional layer of security and protects systems should passwords become known by unauthorized users. • Include controls for encrypted vendor remote access sessions, which is consistent with CIP-005 Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the proposed language meets the requirement of our current SAR. If additional requirements as discussed above were included, it would extend outside the scope of the approved SAR.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	

Document Name	
Comment	
Will inventory lists now be required for Low Impact sites? Based on the current requirements, is it safe to assume that cloud electronic access controls are acceptable for vendor remote access into low impact sites?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that nothing that was added in Section 6 changes the scope of assets that entities were already required to create based on the others sections of Attachment 1.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the TR to reflect the changes in the current draft.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	
Document Name	

Comment	
The most concerning to us is Attachment 1, Section 6.3 in which the term "detecting" known or suspected malicious communications for vendors is used. The term "detecting" is unclear to us. We are unsure if this would require continuous monitoring of the vendor's session, or if it is simply intended to at least manually review the vendor's session after the fact. Is the intent to provide constant real-time monitoring, which would be costly and time consuming?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The current draft language is intended to be risk-based to allow entities flexibility in defining their plans and then implementing the plan as designed.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
With the consideration of the FERC NOPR. Additional architecture diagrams should be illustrated for a possible IDS/IPS implementation similar to when EAC under section 3 there were guidance architecture diagrams.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2016-02 team is preserving the reference documents that were in the GTB of CIP-003-8 in TR documents going forward. The diagrams that reference section 3 still apply to this draft of the standard and any communication crossing those boundaries are still appropriate.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	

Answer	
Document Name	
Comment	
In the Technical Rational, first sentence in the foreward, consider using language consistent with Section 6. Change 'electro nic remote vendor access' to 'electronic vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The TR has been updated to reflect the current draft language.	
Wes DeKemper - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	
Document Name	
Comment	
The Technical Rationale document had a footnote reference to the term vendor as used in CIP-013 that was removed. BHE found it useful and requests that the footnote be reinstated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The TR has been updated to reflect the current draft language.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions | CIP-003-X

Additional Ballot and Non-binding Poll Open through April 15, 2022

Now Available

The additional ballot for **CIP-003-X - Cyber Security — Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Friday, April 15, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Balloting
Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.
For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Extended, Now Open through April 15, 2022

Now Available

The 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls** has been extended and is now open through **8 p.m. Eastern, Friday, April 15, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Commenting
Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps
An additional ballot for the standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 6-15, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/244)
Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 2 ST
Voting Start Date: 4/6/2022 12:01:00 AM
Voting End Date: 4/15/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 237
Total Ballot Pool: 291
Quorum: 81.44
Quorum Established Date: 4/15/2022 2:59:25 PM
Weighted Segment Value: 52.62

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	78	1	32	0.516	30	0.484	0	4	12
Segment: 2	6	0.1	0	0	1	0.1	0	4	1
Segment: 3	70	1	33	0.569	25	0.431	0	2	10
Segment: 4	20	1	7	0.583	5	0.417	0	1	7
Segment: 5	63	1	24	0.511	23	0.489	0	5	11
Segment: 6	47	1	17	0.515	16	0.485	0	3	11
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	1	0	0	0	0	0	0	0	1
Segment: 10	5	0.4	2	0.2	2	0.2	0	1	0
Totals:	291	5.5	115	2.894	102	2.606	0	20	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	American Transmission Company, LLC	LaTroy Brumfield		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Mike Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Taunton Municipal Lighting Plant	Devon Tremont		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Wind Energy Transmission Texas, LLC	doug whitworth		None	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	Portland General Electric Co.	Adam Menendez		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	Wabash Valley Power Association	Susan Sosbe		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	John McCaffrey		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	DTE Energy	patricia ireland		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Evergy	Derek Brown		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Abstain	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young	Helen Zhao	None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Robin Berry		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Marty Watson		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Abstain	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 1 of Pend Oreille County	April Owen		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Santee Cooper	Glenda Horne		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
7	Amazon Web Services	Kristine Martz		None	N/A
9	British Columbia Utilities Commission	Sarosh Muncherji		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X | Non-binding Poll AB 2 NB
Voting Start Date: 4/6/2022 12:01:00 AM
Voting End Date: 4/15/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 227
Total Ballot Pool: 277
Quorum: 81.95
Quorum Established Date: 4/15/2022 3:01:07 PM
Weighted Segment Value: 49.43

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	74	1	26	0.5	26	0.5	11	11
Segment: 2	6	0	0	0	0	0	4	2
Segment: 3	69	1	26	0.531	23	0.469	9	11
Segment: 4	19	0.9	5	0.5	4	0.4	4	6
Segment: 5	59	1	15	0.417	21	0.583	13	10
Segment: 6	44	1	13	0.464	15	0.536	7	9
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	1	0	0	0	0	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	5	0.2	2	0.2	0	0	3	0
Totals:	277	5.1	87	2.612	89	2.488	51	50

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Mike Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Comments Submitted
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Taunton Municipal Lighting Plant	Devon Tremont		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A
1	Wind Energy Transmission Texas, LLC	doug whitworth		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Independent Electricity System Operator	Harishkumar Subramani Vijay Kumar		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	Portland General Electric Co.	Adam Menendez		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		None	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	Wabash Valley Power Association	Susan Sosbe		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	American Public Power Association	John McCaffrey		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	DTE Energy	patricia ireland		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Comments Submitted
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Amanda Wangler		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Abstain	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Marty Watson		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Abstain	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Negative	Comments Submitted
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Glenda Horne		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
9	British Columbia Utilities Commission	Sarosh Muncherji		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 18, 2020
SAR posted for comment	April 8, 2020
45-day formal comment period with ballot	August 27 – October 11, 2021
45-day formal additional comment period with ballot	February 25 – April 15, 2022

Anticipated Actions	Date
45-day second additional formal comment period with ballot	July 6 – August 19, 2022
10-day final ballot	September 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its	approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its	approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning	Lower	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2,	assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low	more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security plan(s) for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity	Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
X	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies (e.g., full packet inspection technologies);
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third 45-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 18, 2020
SAR posted for comment	April 8, 2020
45-day formal comment period with ballot	August 27 – October 11, 2021
45-day formal additional comment period with ballot	February 25 – April 15, 2022

Anticipated Actions	Date
45-day second additional formal comment period with ballot	July 6 – August 19, 2022
10-day final ballot	September 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-X:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. ~~Electronic v~~Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to	containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media	implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented ~~electronic~~vendor electronic remote access security controls but failed to document its cyber security plan(s) for ~~electronic~~vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2,	Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for ~~electronic~~vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for ~~electronic~~ vendor electronic remote access security controls, but failed to implement ~~electronic~~ vendor electronic remote access security controls according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than 40 calendar days of the change. (R4)	in less than 50 calendar days of the change. (R4)	in less than 60 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Version	Date	Action	Change Tracking
X	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. ~~Electronic~~ Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with ~~electronic~~ vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining ~~electronic~~ vendor electronic remote access ~~where such access has been established under Section 3~~;

6.2 One or more method(s) for disabling ~~electronic~~ vendor electronic remote access ~~where such access has been established under Section 3~~; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications. ~~for both inbound and outbound vendor communications.~~

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. ~~Electronic~~ Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - ~~S~~security ~~I~~information ~~M~~management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS,

router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing ~~active~~ vendor electronic remote access;

- disabling communications protocols (such as IP) used for systems which establish and/or maintain ~~active~~ vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable ~~active~~ vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies (e.g., full packet inspection technologies) ~~Firewall policies~~;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - ~~Virtual Private Network (VPN) hosts;~~
   - Automated or manual log reviews; ~~or~~
   - alerting; or
   - other operational, procedural, or technical controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-X — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

Reliability Standard CIP-003-X

[1] See Applicability section of CIP-003-X for additional information on Distribution Providers subject to the standard.

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 36 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is 36 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-X as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-X.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-X within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-X — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

[1] See Applicability section of ~~Revised~~ CIP-~~Standards and Definitions~~-003-X for additional information on Distribution Providers subject to the ~~standards~~standard.

Reliability Standard CIP-003-X

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is ~~18~~36 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-X shall become effective on the first day of the first calendar quarter that is ~~18~~36 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

~~**Compliance Date for CIP-003-X, Requirement R2, Attachment 1, Section 6.3**~~

~~Responsible Entities shall not be required to comply with Requirement R2, Attachment 1, Section 6.3 until six months after the effective date of Reliability Standard CIP-003-X.~~

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-X as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-X.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-X within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2020-03 Supply Chain Low Impact Revisions** by **8 p.m. Eastern, Friday, August 19, 2022.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Questions

1. Do you agree the updated languge proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. The team has added clarifying languge to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT has added clarifying language that limits the scope to Section 3.1. Do you believe the language in Attachement 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT is proposing a 36-month implementation plan for Attachment 1, Section 6 based on industry feedback. Would these proposed timeframes give enough time to put into place process,

procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

☐ Yes
☐ No

Comments:

7. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-X

July 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

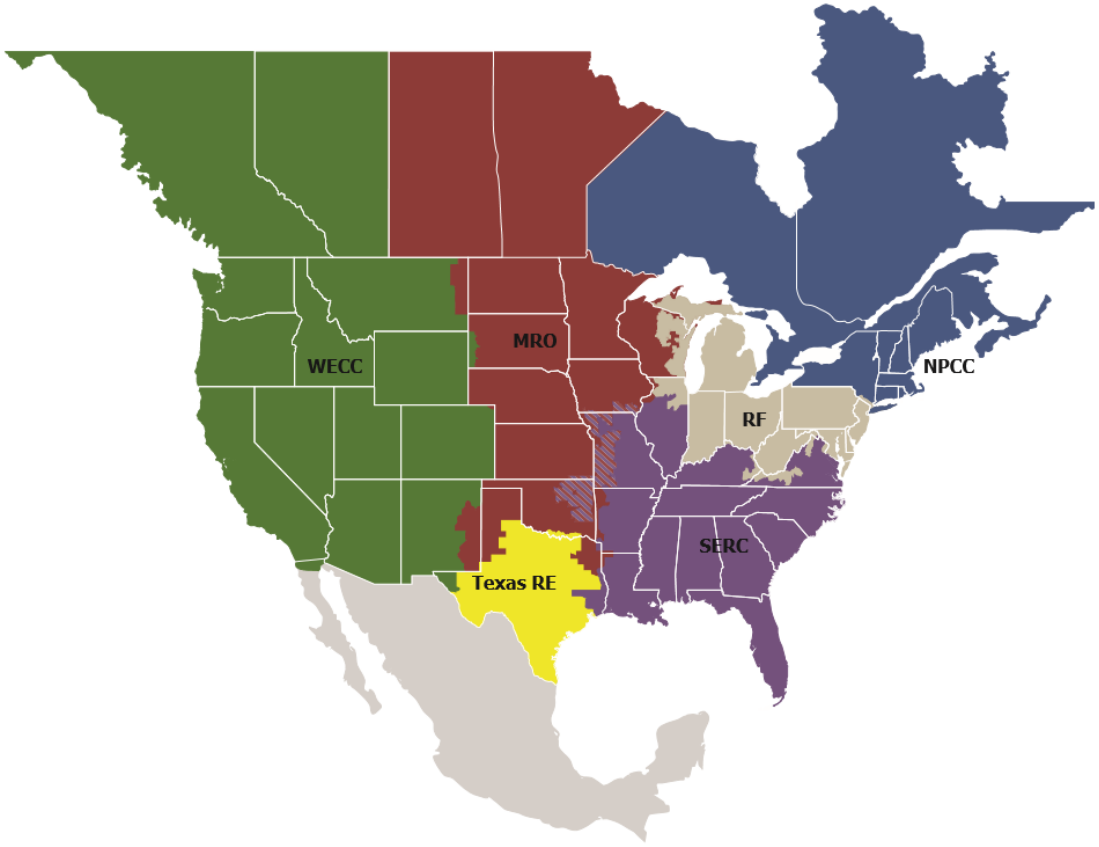
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-X Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

[3] CIP-013 Technical Rationale

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-X Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-X

~~February~~July 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

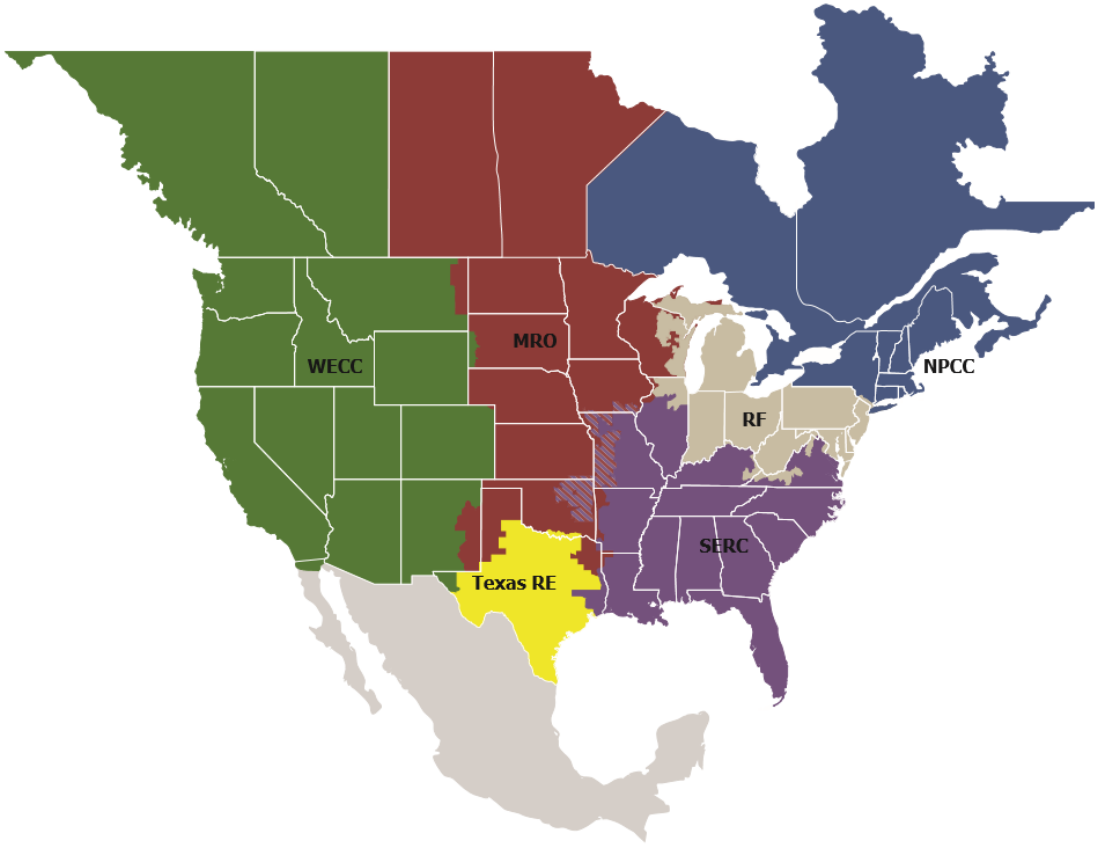
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through ~~MRC Policy Input~~Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT ~~reviewed~~considered many variables and ~~proposed multiple language options~~inputs to ~~clarify the~~ draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of ~~electronic~~entity sizes, functions, organizations, systems and configurations, entity business processes, remote ~~vendor~~ access ~~in context of existing Section 3 electronic access controls. In addition, the SDT considered process considerations, remote and~~, local electronic access, remote access architectures and technologies, and data ~~paths~~path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

~~The SDT agreed to retain Section 3 and establish Section 6 to address vendors and low impact electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors.~~

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL Minutes BOT Open Meeting February 2020.pdf (nerc.com)

entity personnel, or cases where entities use ~~disparate~~separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and ~~cyber assets~~Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and ~~cyber assets~~Cyber Assets owned by entities but used by vendors for electronic remote access.

~~Given these multiple considerations~~Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms defintion in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-X Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic ~~vendor~~ remote access~~ and~~, as well as malicious inbound~~/~~ and outbound ~~malicious~~data communications ~~for low impact.~~ which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic ~~vendor~~ remote access, having a method or methods for disabling vendor electronic ~~vendor~~ remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

~~The language gives entities the flexibility to define processes to identify and manage electronic vendor remote access for their specific policies, processes, systems, configurations, organizations, operations, and Facilities. The language allows entities to define how and where electronic vendor remote access occurs and the ideal methods and timeframes to authorize, establish and disable electronic vendor remote access.~~

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic ~~vendor~~ remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

[3] CIP-013 Technical Rationale

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine ~~when active~~ vendor electronic remote access ~~sessions are~~is initiated; and (3) disable ~~active~~ vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of ~~external connectivity.~~vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement ~~2~~R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic~~vendor~~ remote access.

Attachment 1 Section 6 Part 6.1 – Determining ~~Vendor Remote Access~~vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to ~~have visibility of~~ determine vendor electronic ~~vendor~~ remote access ~~on~~to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have ~~a method to determine~~one or more methods for determining vendor electronic~~vendor~~ remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic ~~vendor~~ remote access ~~in~~for any basis the ~~event of a security event, the inability of a responsible~~ entity ~~to terminate a connection~~ may ~~allow~~choose and to prevent security events and propagation of potential malicious communications which may degrade or ~~otherwise inappropriate communication to propagate, contributing to a degradation of a~~have adverse effects upon the entity's assets containing low impact BES Cyber ~~Asset's function. Enhanced visibility into electronic vendor remote access and the ability to terminate electronic vendor remote access could mitigate such a vulnerability.~~Systems. The obligation in Section 6.2 requires that entities have a method to disable ~~electronic vendor remote access.~~vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications ~~by~~from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub ~~part~~section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current ~~Requirements~~obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact ~~BES Cyber Systems and~~ medium impact BES Cyber Systems. Security controls such as use of ~~intermediate systems~~Intermediate Systems and multi-factor authentication provide ~~high impact BES Cyber Systems and medium impact BES Cyber Systems~~ additional security protection from malicious communication and overall access controls~~.~~ for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high ~~impact BES Cyber Systems~~ and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a ~~Low~~low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security ~~Requirements~~requirements to detect malicious communications under CIP-003-X Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2020-03 Supply Chain Low Impact Revisions

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-003-X. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-003-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR	than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR	than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR

VSLs for CIP-003-X, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-012-2 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was modified by adding a seventh topic to Requirement R1.2 for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to review one or more documented cyber security policies covering the topics specified in Requirement R1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-012-2 Requirements R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-X, Requirement R2

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement	according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR	

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic	authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and	

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
remote access security controls but failed to document its cyber security plan(s) for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security plan(s) for vendor electronic remote access security controls according to	

VSLs for CIP-003-X, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security plan(s) for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	

VSL Justifications for CIP-012-2 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was not modified but the attachment referenced in the requirement was. The attachment was modified by adding a sixth section for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented cyber security plans covering the sections specified in Attachment 1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-012-2 Requirements R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-X, Requirement R3
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R3
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VRF Justification for CIP-003-X, Requirement R4
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-X, Requirement R4
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Open through August 19, 2022

Now Available

A 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls**, is open through **8 p.m. Eastern, Friday, August 19, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 10-19, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2020-03 Supply Chain Low Impact Revisions | Draft 3
Comment Period Start Date:	7/6/2022
Comment Period End Date:	8/19/2022
Associated Ballots:	2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 3 ST

There were 75 sets of responses, including comments from approximately 175 different people from approximately 105 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the updated languge proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The team has added clarifying languge to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT has added clarifying language that limits the scope to Section 3.1. Do you believe the language in Attachement 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT is proposing a 36-month implementation plan for Attachment 1, Section 6 based on industry feedback. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

7. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Carnesi	Chris Carnesi		WECC	NCPA	Marty Hostler	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
Santee Cooper	James Poston	3		Santee Cooper	Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC

					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Ryan Strom	Buckeye	5	RF

						Power, Inc.		
					Colette Caudill	East Kentucky Power Cooperative	1,3	SERC
					Michael Brytowski	Great River Energy	3	MRO
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
LaKenya VanNorman	LaKenya VanNorman		SERC	Florida Municipal Power Agency (FMPA)	Chris Gowder	Florida Municipal Power Agency	5	SERC
					Dan O'Hagan	Florida Municipal Power Agency	4	SERC
					Carl Turner	Florida Municipal Power Agency	3	SERC
					Jade Bulitta	Florida Municipal Power Agency	6	SERC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility	1	WECC

						District No. 1 of Chelan County		
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian	DTE Energy -	5	RF

					Raducea	Detroit Edison Company		
Paul Haase	Paul Haase		WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Harish Vijay Kumar	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power	4	NPCC

	Generation, Inc.		
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
Brian Robinson	Utility Services	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
John Pearson	ISONE	2	NPCC

					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Tim Kelley	Tim Kelley		WECC	SMUD / BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree the updated languge proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The introduction of "detecting known or suspected malicious communications" for low impact BES Cyber Systems would be more stringent as compared to CIP-005 R1.5 since Medium Impact BES Cyber Systems are not applicable in the current version of the standards without adding any additional reliability benefits.

Likes 4	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre; WEC Energy Group, Inc., 3, Kane Christine; Central Hudson Gas & Electric Corp., 1, Ridolfino Michael; Jones Barry On Behalf of: sean erickson, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

As with the previous draft, Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS (i.e., those outside of control centers). Section 6.3 would require detection of malicious inbound and outbound communications for low impact BCS with vendor remote connectivity. In the current version and next effective version of CIP-005, Part 1.5 requires detection of malicious inbound and outbound communications only for medium impact BCS at Control Centers.

BPA recognizes that the NERC Board Resolution directs the drafting team to modify CIP-003 to "..include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications…" BPA also acknowledges that the Technical Rationale attempts to identify more robust controls from CIP-005-6 that offset this inconsistency. However, this inconsistency results in a complicated and confusing compliance approach: entities will be required to develop separate evidence packages for Low and Medium (outside of control centers) substations even if they implement identical solutions across both.

Likes 4	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre; Platte River Power Authority, 6, Martz Sabrina; Platte River Power Authority, 3, Kiess Wade; Wabash Valley Power Association, 3, Sosbe Susan
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

BC Hydro appreciates the opportunity to comment and thanks the drafting team for their continued efforts.

The language proposed in CIP-003-X attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- The language used in CIP-003-X attachment 1 Section 6.3 is referring to 'known or suspected malicious communications'. BC Hydro recommends adding more clarity and provide examples of use cases and applicability. Specifcally, context and usage of the term 'malicious communication' needs more clarity and BC Hydro requests to provide the context and usage with pertinent examples and use case scenarios to improve understanding and to better scope the requirements.
- Similarly, BC Hydro proposes defining and adding term 'Vendor Electronic Remote Access' to NERC Glossary of Terms.
- Who and what is considered a 'Vendor' also need to be defined in the Glossary of Terms for clarity and understanding.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5.

BC Hydro recommends rewording or removing Section 6.3 completely.

Likes 1	Jones Barry On Behalf of: sean erickson, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	

James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Attachment 1 Section 6 was introduced as an objective risk-based requirement; however, it lists prescriptive actions. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection. As such the language should read more like an objective risk-based requirement allowing an entity to have a bit more leeway to comply with the requirements.

Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities

(Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

Tacoma Power does not agree that the proposed language in Attachment 1, Section 6 addresses the risk of malicious communication. The Section 6 introduction includes an objective risk-based high-level requirement, yet prescriptive actions are listed in the sub-parts. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection.

Tacoma Power suggests the following wording to avoid prescriptive language in the sub-parts (changes noted in italics and important word changes are highlighted with bold text):

Section 6**:** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall ***address*****:**

6.1 determining and disabling ***active*** *vendor electronic remote access sessions,* ***if applicable****; and*

6.2 malicious communications.

By altering the wording as shown above, an entity would be able to comply through multiple means and would not HAVE to implement a detection method to mitigate malicious communication. For example, if an Entity makes use of an Intermediate System for all low impact BCS remote access, which would mitigate the risk of vendor electronic remote access malicious communications, they have addressed malicious communications without having to also detect malicious communications, which in this scenario is extremely unlikely to occur.

Likes 3	Platte River Power Authority, 6, Martz Sabrina; Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE continues to be concerned that the language in Attachment 1, Section 6 is limited to vendor remote access. Texas RE is concerned that Section 6's focus on vendor remote access does not capture the full range of malicious communications contemplated under the low impact guidance documents. In the event of a supply chain attack, malicious communications can occur whether or not a Responsible Entity has established an authorized channel for vendor communications. Additionally, in the event of a supply chain attack, malicious communications can potentially be initiated from compromised Cyber Assets attempting to communicate with a Command and Control server. Importantly, these can occur along logical pathways for which where the Responsible Entity has deliberately not established channels for vendor remote access.

A supply chain attack, such as the supply chain attack that resulted in the 2020 United States federal government data breach, is not typically conducted directly by compromised vendors themselves. These attacks are typically conducted by malicious third parties that do not have a formal business relationship with the vendor or the affected Registered Entity. As such, scoping this requirement to only address remote access that is conducted directly by vendors would deliberately exclude from scope the exact communications that need to be monitored.

Based on this perspective, therefore, Texas RE recommends that the SDT clarify that CIP-003 low impact monitoring obligations extend to all inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of authorized vendor remote access. Texas RE recommends moving the proposed language in Attachment 1, Section 6.2 to Section 3 (Electronic Access Controls) so it is clear malicious communication monitoring and detection method obligations apply to all communications, not simply vendor remote access communications.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Since Section 6 has introduced an objective risk-based high-level requirement, yet prescriptive actions are listed. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT align the CIP-003 Attachment 1 Section 6 language with CIP-005-6 R2 and use NERC-defined terms where possible. The content of Section 6 should be included within Attachment 1 Section 3 and not made into a new section. Reclamation recommends adding “if technically feasible” to Section 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

Reclamation recommends the following changes to Section 6:

From:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

To:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for identifying active vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling active vendor remote access.

The phrase “determining active vendor remote access sessions” is not clear. Reclamation recommends using the same language as in the Technical Rationale, which refers more specifically to ”when sessions are initiated.”

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

SMUD and BANC support Tacoma Power's comment.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS (i.e., those outside of control centers). It is still not clear is VPN connections established with support vendors fully adheres to requirement or additional steps such as IDS/IPS are required. The Section 6 introduction includes an objective risk-based high-level requirement, yet prescriptive actions are listed in the sub-parts.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
NCPA does not agree with prescriptive language for 6.3 as it relates to detect known or suspected malicious communications. This would be more arduous for Low impact entities to implement compared to non-Control Center Medium Impact facilities as they don't need to comply with CIP-005 R1.5. This creates an imbalance of requiring lower risk facilities to comply with a more strenuous requirement than higher risk facilities. At least limiting 6.3's scope to only Low Impact Control Centers would be somewhat congruent with the CIP-005 R1.5 requirement.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment

Malicious communication can arguably be effectively addressed with Attachment 1, requirements 6.1 and 6.2. We believe that Requirement 6.3 is excessive.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

It is not clear that Section 6.3 only applies to only inbound and outbound vendor communication and not all communication established under Section 3.1. If Section 6.3 is applicable to all communications then it should be moved to Section 3.1.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Based on the comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD does not agree that the proposed language in Attachment 1, Section 6 addresses the risk of active malicious communications and is too prescriptive in the actions listed in Section 6.1 – 6.3. Entities can mitigate the risks associated with vendor electronic remote access through various means and still address the NERC Board Resolution to detect, determine, and disable active vendor electric remote access, and malicious communications. The language should read more like an objective risk-based requirement allowing an entity to have a bit more leeway to comply with the requirement. Additionally, as written Section 6.3 appears to be applicable to all communications and should then be removed from Section 6.3 and	

placed in Section 3.1 if this was the intent.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy supports the comments of EEI and the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees that the proposed language in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impace BES cyber systems as directed by the NERC Board resolution.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E agrees the updated language in Attachment 1, Section 6 addresses the risks noted by the NERC Board of Trustees resolution.

Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI agrees that the updated language proposed in Draft 3 of Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Yes, Constellation agrees the the updated language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Yes, Constellation agrees the the updated language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems.

Kimberly Turco on behalf of Constellation Segements 5 and 6

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster

Answer	Yes
Document Name	

Comment

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #1.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Minnesota Power is in agreement with EEI's comments.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	Yes

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While the language added to the standard does meet the NERC Board resolution, we still strongly disagree with adding malicious code detections for low impact BCS (specifically Section 6.3) as this control is not a requirement for medium impact BCS (not at Control Centers). Although these new requirements come from the FERC/NERC resolution, there are much greater risks to the overall BES/BPS, at medium impact BCS than low impact BCS. We feel the only resolution to this, is to add the same controls to medium impact BCS or drop the requirement for low impact. If we as an ERO are taking a risk based approach and the FERC/NERC resolution into consideration, then adding the requirement to medium impact BCS is the only possible resolution to satisfy us and the FERC/NERC resolution. Based on our research there is not a resolution to add malicious code detections to medium impact BCS and therefore we will not be in favor of the controls for low impact.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the updated language proposed in Draft 3 of Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form (GSOC FINAL).docx
Comment	
GSOC believes the updated language in section 6 addresses the risk; however modifications to section 6.3 introduce confusion regarding the scope of the requirement over the last posting by arguably including non-vendor related communications in the language. This broadening of language could be read to include asset-level monitoring of all inbound and outbound communication for known or suspected malicious communications is a significant departure from the previous draft and would result in an unduly burdensome compliance mandate. The Technical Rationale developed by the SDT states that section 6.3 "is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report." However, the SDT has removed the language from 6.3 that clarifies this scope. Since the SDT moved the language that states "where such access has been established under Section 3.1" to the main part of Section 6, this language could be read as requiring this detection to occur at the point where access is established under Section 3.1 which defines that access at each asset containing low impact assets. Further, 6.3 could be read to require all malicious communications to be detected, regardless of whether it is vendor communication or not as there is no reference to vendor communication in the control specified in section 6.3.	

GSOC respectfully proposes the following wording that reverts the language in 6.3 to the language of the prior posting:

Vendor Electronic Remote Access Security Controls: For assets containing

low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible

Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.

These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote

access;

6.2 One or more method(s) for disabling vendor electronic remote

access; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	Yes
Document Name	

Comment

ITC is in agreement with the EEI response

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	Yes
Document Name	

Comment

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rob Watson - Choctaw Generation Limited Partnership, LLLP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	

Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	

2. The team has added clarifying languge to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Deanna Carlson - Cowlitz County PUD - 5

Answer	No
Document Name	

Comment

Cowlitz PUD would like to see the terms 'vendor electronic remote access'; added to Section 6.3 as it is included in Section 6.1 and 6.2. By excluding this from Section 6.3 an interpretation could be applied to malicious communications more broadly than as was intended.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

See comments as supplied by Deanna Carlson from Cowlitz PUD.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

The CIP Standards use many terms:

Vendor electronic remote access (proposed CIP-003)

Inbound and outbound electronic access (CIP-003, Section 3)

User-initiated interactive access (CIP-003 Reference Model 5)

Indirect access (CIP-003 Reference Models 6 and 9)

Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The CIP Standards use many terms such as: Vendor electronic remote access (proposed CIP-003), Inbound and outbound electronic access (CIP-003, Section 3), User-initiated interactive access (CIP-003 Reference Model 5), Indirect access (CIP-003 Reference Models 6 and 9). Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC believes the updated language in section 6, specifically section 6.3 does not clarify the scope of the requirement. The language that provided that clear scoping was removed in this posting. Section 6.3 could now be read to require all malicious communications to be detected, regardless of whether it is vendor communication or not as there is no reference to vendor communication in the control specified in section 6.3. GSOC respectfully proposes the following wording which reverts the language in 6.3 to that of the prior posting:

Vendor Electronic Remote Access Security Controls: For assets containing

low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible

Entity shall implement a process to mitigate risks associatedwith vendor electronic remote access, where such access has been established under Section 3.1.

These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote

access;

6.2 One or more method(s) for disabling vendor electronic remote

access; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren believes the term vendor needs to be more defined more clearly. Does the vendor role make a difference (contractor operators, support, etc.)? Is operations different from support in terms of vendors?

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

The second paragraph of Attachment 1 states “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s).” It is unclear how this statement can be applied without clarification on how the terms used in CIP-005-7 relate to the proposed terms in CIP-003-x. Request clarification on how the CIP-003-X term “vendor electronic remote access” relates to the CIP-005-7 terms “active vendor remote access” (R2) and “vendor-initiated remote connections”(R3).

The CIP Standards use many terms:

· Vendor electronic remote access (proposed CIP-003)

· Inbound and outbound electronic access (CIP-003, Section 3)

· User-initiated interactive access (CIP-003 Reference Model 5)

· Indirect access (CIP-003 Reference Models 6 and 9)

Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment

Please define if “Vendor Electronic Remote Access” is only for Interactive Access or does it include system to system access as well.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

The CIP Standards use many terms:

{C}· Vendor electronic remote access (proposed CIP-003)

{C}· Inbound and outbound electronic access (CIP-003, Section 3)

{C}· User-initiated interactive access (CIP-003 Reference Model 5)

{C}· Indirect access (CIP-003 Reference Models 6 and 9)

Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	

Response
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment
SMUD and BANC support Tacoma Power's comment.

Likes 0	
Dislikes 0	

Response
Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment
Reclamation recommends adding “Vendor” to the NERC Glossary of Terms and proposes the following definition: Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts to supply equipment for BES Cyber Systems and related services. Vendor does not include other NERC-registered entities that provide reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). Vendor may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Likes 0	
Dislikes 0	

Response
Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
While the high-level Section 6 introduction includes scoping language, the wording of the sub-parts 6.1 & 6.2 include the same vendor electronic remote access language, while 6.3 does not. Sub-part 6.3 may be construed to apply more broadly due to the omission of the scoping language in this sub-

part, because the other sub-parts include this scoping language. PGS recommends including the language “vendor remote access”.	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	No
Document Name	
Comment	
Sections 6.1 and 6.2 use the terms ‘vendor electronic remote access’; however, Section 6.3 does not use this language which could lead to confusion for utilities. Even though the high level Section 6 limits the scope to remote access conducted by vendors, Section 6.3, without having the same language as Sections 6.1 and 6.2, could be interpreted to apply to malicious communications more broadly and not just for vendor electronic remote access. Suggested language: In Section 6.3, instead of saying “One or more method(s) for detecting known or suspected inbound and outbound malicious communications,” the suggested language is as follows: “One or more method(s) for addressing and mitigating known or suspected inbound and outbound malicious communications for vendor electronic remote access"	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
While the high-level Section 6 introduction includes scoping language, the wording of the sub-parts 6.1 and 6.2 include the same vendor electronic remote access language, while 6.3 does not. Sub-part 6.3 may be construed to apply more broadly due to the omission of the scoping language in this sub-part, because the other sub-parts include this scoping language. Tacoma Power recommends including the “vendor remote access” language to the sub-part 6.3 sentence, in accordance with the the following Westlaw reference: https://content.next.westlaw.com/practical-law/document/Ibe943df6e1e711e698dc8b09b4f043e0/Expressio-unius-est-exclusio-alterius?viewType=FullText&transitionType=Default&contextData=(sc.Default)&firstPage=true	
Likes 2	Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The term “vendor” needs to be defined in the NERC glossary of terms. The use of the term “vendor” in the CIP-013 Supplemental Material is not an official definition. This term is crucial to CIP-013 and with the proposed changes to CIP-003 the term will be crucial in determining what is considered vendor remote access.	
Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As mentioned in comments related to Question 1 above, 'vendor electronic remote access' needs clarity of understanding and clear definitions of the terms for appropriate applicability as well as the use of term 'Vendor' e.g., whether a consultant using same infrastructure is considered vendor.	
Likes 0	
Dislikes 0	

Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	

Response

LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)

Answer	Yes
Document Name	

Comment

We appreciate the time and attention the SDT put forth working on this section, however we are concerned that the language under 6.3 does not include a direct reference to “vendor remote accesss” in the sub part. We understand the SDT debated this issue, however we recommend modification to the language to improve clarity. We believe these clarifications can be made without substantial change, so are thereby voting affirmative with the desire for futher clarification. These are possible improvements to the language:

1) Adding clarity to the last sentence of section 6:

"These vendor electronic remote access processes shall include:" By adding "vendor electronic remote access", it helps clarify the intent of all three sub-sections being applicable to just "vendor electronic remote access" and not all communications. While technically the word "these" refers to the previous sentence, we feel there could be more calrity to assist Responsisble Entities to focus on the subject of the revisions.

2) Remove references to “vendor remote access” in 6.1 and 6.2

3) Modifying 6.3 to include a reference to vendor electronic remote access. If 6.3 were modified, we recommend it to read:

“6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications associated with vendor electronic remote access.”

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	Yes
Document Name	

Comment

ITC is in agreement with the EEI response

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the Draft 3 language believing that it is sufficiently clear to limit the scope for remote access to low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes

Document Name	

Comment

We appreciate the time and attention the SDT put forth working on this section, however we are concerned that the language under 6.3 does not include a direct reference to “vendor remote accesss” in the sub part. We understand the SDT debated this issue, however we recommend modification to the language to improve clarity. We believe these clarifications can be made without substantial change, so are thereby voting affirmative with the desire for futher clarification. These are possible improvements to the language:

1) Adding clarity to the last sentence of section 6:

"These vendor remote access processes shall include:" By adding "vendor remote access", it helps clarify the intent of all three sub-sections being applicable to just "vendor remote access" and not all communications. While technically the word "these" refers to the previous sentence, we feel there could be more calrity to assist Responsisble Entities to focus on the subject of the revisions.

2) Remove references to “vendor remote access” in 6.1 and 6.2

3) Modifying 6.3 to include a reference to vendor remote access. If 6.3 were modified, we recommend it to read:

“6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications associated with vendor remote access.”

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
I believe the language is clear however the level of monitoring is not reduced.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #2.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Yes, Constellation believes that the language is clear.

Kimberly Turco on behalf of Constellation Segements 5 and 6

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Yes, Constellation believes that the language is clear.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

NextEra Energy supports EEI's comment: EEI supports the Draft 3 language believing that it is sufficiently clear to limit the scope for remote access to low impact BES cyber systems.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	
Comment	
PG&E agrees the language is clear that remote access is only for vendors.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
I believe the language is clear however the level of monitoring is not reduced.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern believes the language added is clear to limit the scop of remote access conducted by vendors.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light
Answer	
Document Name	
Comment
Seattle City Light abstains
Likes 0	
Dislikes 0	
Response
Gail Golden - Entergy - Entergy Services, Inc. - 5
Answer	
Document Name	
Comment
The technical rationale explains that Section 6.3 is specific to vendor only communication. It would aid the reader's understanding if this is clarified in the actual CIP-003-X standard language.
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	
Document Name	
Comment
As noted in its response to Question 1 above, Texas RE continues to believe that the low-impact standards being developed should not be limited solely to vendor communications. However, if the SDT elects to limit the focus of these requirements solely to vendor communications, Texas RE notes that because the SAR specifically states that CIP-003-8 should be revised to include policies for low impact BES Cyber Systems at locations that allow vendor remote access, Texas RE recommends including “at locations that allow vendor remote access” in Section 6 as well.
Likes 0	
Dislikes 0	

Response

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The use of word "Remote" will need some clarification and perhaps a definition in the defined terms, e.g., how the "Remote" term will be used in the sample scenarios below:
1) On site, but electronically remote (i.e. has to go through EAP despite being at the station).
2) A "vendor" at the work location of Responsible Entity, also electronically remote (i.e. going through EAP).
3) "Traditionally" remote, off site, and electronically remote (also going through EAP).

Likes 0	
Dislikes 0	

Response

Claudine Bates - Black Hills Corporation - 1,3,5,6

Answer	No
Document Name	

Comment

The language says "electronic remote access" it does not state "remote locations," which is appropriate based on the guidance given for CIP-005, which made it clear that "remote access" may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn't matter, only the method used to access the BCS.

Likes 0	
Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 1,3,5,6

Answer	No
Document Name	

Comment

The language says "electronic remote access" it does not state "remote locations," which is appropriate based on the guidance given for CIP-005, which made it clear that "remote access" may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn't

matter, only the method used to access the BCS.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1,3,5,6

Answer	No
Document Name	

Comment

The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.

Likes 0	
Dislikes 0	

Response

Ron Wilgers - Black Hills Corporation - 3 - WECC

Answer	No
Document Name	

Comment

The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC believes the updated language in section 6, specifically section 6.3 does not specifically limit the scope of the requirement to vendor access and communications. GSOC respectfully proposes the following wording:

Vendor Electronic Remote Access Security Controls: For assets containing

low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible

Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.

These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote

access;

6.2 One or more method(s) for disabling vendor electronic remote

access; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request clarification on why Attachement 1, 6.3 does not use the phrase "vendor electronic remote access" while Section 6 and, 6.1 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Request confirmation that the SDE expects all of Attachement 1, Section 3.1 to be in place before Section 6 requirements. If section 3.1 is not met, then Section 6 does not apply.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2, and 6.3.

Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.

Likes 0	

Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
The language says, “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
The language in Section 6, ‘where such access has been established under Section 3.1’ implies the entity is not required to implement a process to ‘mitigate risks associated with vendor electronic remote access’ unless remote access has been (or will be) established. We believe this is appropriate, where entities have opted to categorically deny all electronic remote access to vendors.	
Likes 0	

Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
The language is clear for Section 6.1 and 6.2 that it clarifies this section is specific for Vendor Electronic Remote Access. Section 6.3 could be somewhat ambiguous and may be read to include more than vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications to Attachment 1, Section 6 and those modifications clearly indicate it is for vendor access from a remote location.	
Likes 0	
Dislikes 0	

Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
The wording in sub-parts 6.1 & 6.2 include the same “vendor electronic remote access” language, while subpart 6.3 does not. Sub-part 6.3 should read the same as sub-parts 6.1 & 6.2 so as not to imply that 6.3 should be more broadly enforced beyond its intended purpose.	
Likes 1	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre
Dislikes 0	

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI’s comment: EEI agrees that Attachment 1, Section 6 clarifies that vendor’s access to low impact assets containing BES cyber systems is limited to remote locations.	
Likes 0	
Dislikes 0	

Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Yes. The SDT clarified that Attachment 1 Section 6 only applies to vendor access to low impact assets containing BES cyber systems from remote (off-site) locations. Kimberly Turco on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Yes. The SDT clarified that Attachment 1 Section 6 only applies to vendor access to low impact assets containing BES cyber systems from remote (off-site) locations. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Minnesota Power is in agreement with EEI's comments.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	Yes
Document Name	

Comment

See comments under question 2 to help clarify this.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees that Attachment 1, Section 6 clarifies that vendor's access to low impact assets containing BES cyber systems is limited to remote locations.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	

Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	

4. The SDT has added clarifying language that limits the scope to Section 3.1. Do you believe the language in Attachement 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Deanna Carlson - Cowlitz County PUD - 5

Answer	No
Document Name	

Comment

Additional clarification needs to ensure that the scope of Section 6 applies only to low impact BES Cyber Systems where vendors are actually given remote access. The language as written can be interpreted that all low impact BES Cyber System that are identified in Section 3.1 should have a process in place to detect, determine, and disable active vendor electric remote access, and malicious communications, regardless of vendors having remote access or not.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.

Request clarification on how Sections 3.1 and 6 impact the VSLs.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request confirmation that the SDT expects all of Attachement 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply. Request clarification on how Sections 3.1 and 6 impacts the VSLs.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.

Request clarification on how Sections 3.1 and 6 impact the VSLs

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA

Answer	No
Document Name	

Comment

NCPA does not agree with prescriptive language for 6.3 as it relates to detect known or suspected malicious communications. This would be more arduous for Low impact entities to implement compared to non-Control Center Medium Impact facilities as they don't need to comply with CIP-005 R1.5. This creates an imbalance of requiring lower risk facilities to comply with a more strenuous requirement than higher risk facilities. At least limiting 6.3's scope to only Low Impact Control Centers would be somewhat congruent with the CIP-005 R1.5 requirement.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	
Comment	

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote access' however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5.

BC Hydro recommends rewording or removing Section 6.3 completely.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	
Comment	

There is confusion with the language used in Section 6 as to whether it pertains to the assets containing the low impact BES Cyber Systems (which may contain out of scope cyber systems) or the low impact BES Cyber Systems themselves.

Likes 0	
Dislikes 0	
Response	

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	Yes
Document Name	
Comment	

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	
Response	

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	
EEI agrees that the proposed language in Section 6 limits that scope to Section 3.1.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
The proposed changes to limit scope are redundant. Section 3.1 and Section 6 are explicit to low impact BCS. If vendor remote access wasn't already established and allowed under Section 3.1, there would either be a violation of Section 3.1 or a CIP exceptional circumstance would need to be declared. The language is fine, but unnecessary to try to confine the scope of Section 6 as it is very explicit to low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #4.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	

Answer	Yes
Document Name	
Comment	
Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI agrees that the proposed language in Section 6 limits that scope to Section 3.1.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the modification to Section 3.1 make it clear the scope of the Requirement is for low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	

5. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The scope should be narrowed to just where the risk exists as opposed to a broad swath of assets. The way it is written it implies that all communications need to be monitored to determine malicious communications through vendor remote access.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Although the cost may differ between entities, BC Hydro's assessment is that the impact may change based on understanding & clarity of terms and scope of application. As advised in comments of Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However requirement in CIP-003-X Section 6.3 applies to 'Low Impact BCS' which is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5, where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS out of scope.

Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Including a more restrictive prescriptive control for malicious communication detection for low impact BCS that does not exist for medium impact BCS not at a Control Center is not a cost-effective approach. Medium impact BCS not at a Control Center must still follow CIP-005 R2 for remote access through an intermediate system. This was mentioned as justification for including Section 6.3 for low impact but not requiring for Medium impact BCS not at a Control Center. If an entity implements CIP-005 R2 Intermediate Systems for low impact, they will still not be compliant with CIP-003, Attachment 1, Section 6.3 as currently worded.

In order to provide a more cost effective solution, Tacoma Power suggests that an entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection.

Suggested wording to avoid prescriptive language and provide a more cost effective solution:

Section 6**:** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall ***address*****:**

6.1 determining and disabling ***active*** *vendor electronic remote access sessions,* ***if applicable****; and*

6.2 malicious communications.

Likes 2	Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response

John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC

Answer	No
Document Name	

Comment

Section 6.3 is written in prescriptive way toward only one of many possible solutions for addressing malicious communications. This does not allow entities to analyze and choose the most cost effective approach to addressing and mitigating malicious communication.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Including a more restrictive prescriptive control for malicious communication detection for low impact BCS that does not exist for medium impact BCS

not at a Control Center is not a cost-effective approach. Medium impact BCS not at a Control Center must still follow CIP-005 R2 for remote access through an intermediate system. This was mentioned as justification for including Section 6.3 for low impact but not requiring for Medium impact BCS not at a Control Center. If an entity implements CIP-005 R2 Intermediate Systems for low impact, they will still not be compliant with CIP-003, Attachment 1, Section 6.3 as currently worded.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends Project 2016-02 is a good avenue to incorporate low impact requirements into the CIP standards and avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

SMUD and BANC support Tacoma Power's comment.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	
Comment	
We do not have enough information at this time to address cost-effectiveness of the revisions.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
Cost effectiveness of Attachment 1, 6.1, 6.2, and 6.3 is unknown at this time since the capability will require a technical solution not currently in place. Further, this requirement is not consistent with current CIP-005-6 and future CIP-005-7 enforceable requirements.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
There is a high probability that new technology controls will be required to meet the new requirements. Entities would need to allocate funds and projects to implement new technologies.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No

Document Name	
Comment	
There is a high probability that new technology controls will be required to meet the new requirements. Entities would need to allocate funds and projects to implement new technologies.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

The scope should be modified to read more like an objective-based requirement allowing entities more leeway and potentially more cost-effective means to comply with the specific list of assets identified. Recognition that not all communications need to be monitored to determine malicious communications through active vendor remote access will ensure resources are focused on actual risk.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy agrees that the modifications can be implemented in a cost-effective manner when implemented within the timeframe identified in the associated Implementation Plan.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

Until an approved Standard is in place, PG&E cannot make a determination if the modification are cost effective.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

It is cost effective, but these costs will be pushed directly to ratepayers which requires FERC support to answer the ratepayers.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	Yes
Document Name	

Comment

We requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Minnesota Power is in agreement with EEI's comments.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	Yes
Document Name	

Comment

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST abstains.	
Likes 0	
Dislikes 0	
Response	

Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	

Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	
Document Name	
Comment	
NextEra Energy is not supplying a position nor comment on cost effectiveness of these changes.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation will not comment on cost. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	

Answer	
Document Name	
Comment	
Constellation will not comment on cost. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
Unable to justify cost effectiveness at this time	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost-effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	

Comment	
Once again, we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	
Comment	
Once again, we requested a redline to the last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances of approval. Otherwise, TFIST abstains from commenting on cost effective.	
Likes 0	
Dislikes 0	
Response	

Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light

Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing a 36-month implementation plan for Attachment 1, Section 6 based on industry feedback. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment

It is difficult to estimate as the scope of 6.3 is not clear yet.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

While WECC does not believe the extended 36-month Implementation Plan is reason to vote NO, we believe that considering the risks that are facing the system, the DT should consider moving the Implementation back to 24 months as was included in earlier versions of the draft standard. However, if a 36-month Implementation Plan is what is necessary to gain approval of the Standard, WECC understands.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro recommends a longer implementation plan, e.g. more than ~36 months, considering the cost and scope impact as identified in comments to Question 1 and 4 above. Once the clarity of terms and definitions is obtained as identified in comments to Question 1 and 4, BC Hydro will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

Large entities with hundreds of low impact facilities will need more implementation time for addressing the changes applicable to low impact assets. Suggested timeline is a 5 year plan, implementing 20% of the assets per year.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	Yes
Document Name	

Comment

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5

Answer	Yes
Document Name	

Comment

Cowlitz PUD, Segment 5 8/19/2022

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

We agree with 36 months.

Request deletion of the following language because this language refers to a removed Section – “Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.”

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

Agree with 36-months. Request deletion of the following language because this language refers to a removed Section - "Where the standard drafting team identified the need for a longer implementation period for compliance with a particualar section of a proposed Reliability Standard (i.e., and entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard does into effect at an earlier date."

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	Yes
Document Name	

Comment

ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed 36-month implantation plan for attachment 1, Section 6.	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy thanks the Standard Drafting Team for this important revision. We fully support the proposed implementation timeline.	
Likes 0	
Dislikes 0	

Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the SDT's proposed implementation timeframe recommendation.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
We agree with 36-months. Request deletion of the following language because this language refers to a removed Section – "Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date."	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Increasing the implementation time from 18 to 36 months should allow adequate time for implementation.	
Likes 0	

Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Risk: Supply chain risk to be taken into factor.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #6.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Yes. The proposed 36 months would give enough time to put the process, procedures and technology in place to meet the proposed language in Section 6. Kimberly Turco on behalf of Constellation Segements 5 and 6	

Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Yes. The proposed 36 months would give enough time to put the process, procedures and technology in place to meet the proposed language in Section 6. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI supports the proposed 36-month implantation plan for attachment 1, Section 6.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the 36-month implementation plan and that it would be sufficient time for PG&E to implement the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Increasing the implementation time from 18 to 36 months should allow adequate time for implementation.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and supports the proposed 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the 36 calendar month implementation.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	

We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	

7. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

NST believes redline versions of-proposed Standards should be markups to "last approved," not markups to previous proposed versions. The practice of redlining previous drafts makes it difficult to compare proposed new or modified requirement language to current, in-effect requirements.

NST believes the SDT should, in addition to addressing the NERC Board resolution, revise CIP-003 Requirement R2 to state that documented cyber security plan(s) for a Responsible Entity's low impact BES Cyber Systems are required to address Attachment 1 Sections 3, 5, and 6 only if the following conditions exist:

For Section 3, only if one or more of the Responsible Entity's assets that contain low impact BCS has external connectivity of a type that matches the descriptions in Sections 3.1 and/or 3.2.

For Section 5, only if TCAs and RMs are used at one or more of the Responsible Entity's assets that contain low impact BCS and are occasionally connected to BCS.

For Section 6, only if (a) Section 3.1 is applicable and (b) vendor remote access is permitted.

A Responsible Entity with no vendor remote access should not be expected to document how it addresses Section 6 requirements.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	
Document Name	

Comment

We appreciate the time and level of effort that the Drafting Team has put in to address the many concerns related to vendor access to Low Impact Cyber Systems. Their efforts will eventually result in modifications to CIP-003 that will benefit the industry, protect the Bulk Electric System, and better serve the ratepayers.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE recommends the following revisions be made to the CIP-003-X Technical Rationale document for clarity:

1. Define the acronym “SAR” as “Standard Authorization Request” and

2. On page 5, under “1. Electronic remote access:”, add a statement to clarify that “electronic remote access” includes interactive and system-to-system remote access.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	

Attachment 1, Section 6, sub-section 3. The wording is good but can further be clarified by adding “for vendor electronic remote access” to the end:

One or more method(s) for detecting known or suspected inbound and outbound malicious communications **for vendor electronic remote access**.

Attachment 2, Section 6, sub-section 3. (examples of evidence) the wording is good but can further be clarified:

Network based Anti-malware technologies such as deep packet inspection;

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS); or

Automated or manual log reviews; or

Automated User Behaviour Analytics (UBA); or

SIEM network traffic or vendor remote access log analysis and alerting; or

other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	
Document Name	
Comment	
In the Consideration of Comments document for the Draft 2 ballot, the SDT states that "…the SDT believes "remote access" is any access that crosses this boundary (Attachment 1 Section 3.1). If a vendor is "onsite" but starts the connection process outside this boundary, this connection should be considered remote access." CHPD believes that by including this statement in the Technical Rational document it will provide stakeholders and the ERO Enterprise with a better understanding of the requirements in the CIP-003-X Reliability Standard.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	

Consider updating Section 6.3 to be more clear in identifying the language is specifically geared towards Vendor Electronic Remote Access **only**.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro ackowledges the SDT's effort and hard work which went into putting together these complex changes to CIP-003-X. As identified in comments of question 1 to 4 above, the definitions of terms and clarity of application with some specific industry use case examples will help providing a more clear understanding and likely result in a faster and appropriate approvals of these proposed changes.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E wishes to thank the SDT for listening to the industry’s input and the effort in making these modifications to address the NERC Boards resolution

Likes 0	
Dislikes 0	

Response

Claudine Bates - Black Hills Corporation - 1,3,5,6

Answer	
Document Name	

Comment

n/a	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	
Document Name	

Comment

NextEra Energy thanks the SDT for its service of improving the security of the bulk electric system.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	
Document Name	

Comment

Constellation does not have any additional comments.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	
Document Name	

Comment

Constellation does not have additional comments.

Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	
Document Name	
Comment	
Even though Attachment 1, Section 6 addresses the risk of malicious communication, it does so in a prescriptive way in that the standard is directing utilities toward a particular solution (e.g. detecting with software/hardware or detection processes) rather than allowing the utility to choose the best approach/method to address and mitigate malicious communication.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
In Attachment 1, Section 6, Texas RE recommends specifying “pursuant to CIP-002” rather than referencing another NERC Reliability Standard, as requirements should be complete and self-contained as noted in the Ten Benchmarks of an Excellent Reliability Standard. Texas RE recommends the following language: “For each asset that contains a low impact BES Cyber System, and for which the Responsible Entity allows vendor remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access.” Additionally, Texas RE recommends the SDT Include language for (1) software integrity and authenticity, (2) information system planning, and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010.	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	
No additional comments at this time. AEP thanks the SDT for their efforts on this draft.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	

Document Name	
Comment	
BHE requests the words “and timeframes [keep the “to”] authorize,” be removed from the Technical Rationale, page 5: “The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.” BHE is concerned this reference to timeframes and authorization could lead Regional Entities to question both, when neither appear in the 6.1 obligation to determine access. BHE also recommends for Attachment 2, Section 6.3, to lowercase “Intrusion Detection System/Intrusion Prevention System” since it’s not a glossary term and not a formal name. Thanks to the SDT for the fine work on this standard.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
With the consideration of the FERC NOPR. Additional architecture diagrams should be illustrated for a possible IDS/IPS implementation similar to when EAC under section 3, there was guidance architecture diagrams.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
None. Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
Is the intent of this section to not include dial-up? If so, it would be better to clarify in the language.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	

we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.

Request consistency the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.”

Recommend consistency between Attachment 1, Section 6 and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one of more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:”

Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for medium impact that is not at a Control Center.

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or

leaving an ESP." 6.3 says "One or more method(s) for detecting known or suspected inbound and outbound malicious communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers.

Request clarification on why Attachment 1, 6.3 does not use the phrase "vendor electronic remote access" while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

The NAGF requests the SDT to consider adding language in Attachment 2 Section 6.3 to clarify that documentation of vendor contractual agreements to maintain malicious communication security controls would be an appropriate approach to meet compliance with Attachment 1 Section 6.3.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	
Document Name	

Comment

Like NAGF, Duke Energy asks the Standard Drafting Team to consider adding language in Attachment 2 Section 6 Part 3 to explicity clarify that documentation of vendor contractual agreements to maintain malicious communication security controls could be an approach to comply with Attachment 1 Section 6.3. Without this addition, compliance with the revisions could be challenging for OEM connections, given that many vendors consider their communications with covered equipment to be proprierty information or intellectual property that they are not willing to have inspected.

We also recommend that the Drafting Team reconsider the one example in Attachment 2 Section 6 Part 3 where it says "anti-malware technologies e.g. full packet inspection." We would either like to see the one example taken away, or more added, since one example could imply one best option.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Section 6 states “the Responsible Entity shall implement a process“while CIP-003-XR2, for which Section 6 is dependent, requires the implementation of a plan. The second paragraph in Attachment 1 states “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s).” Additionally, Attachment 2, Section 6 states “For Section 6.3, documentation showing implementation of processes or technologies”. The VSL related to Section 6 only references a “plan”. Suggest removing the requirement to use a “process” from Attachment 1 section 6. Additionally, suggest that the language of Attachment 1 Section 6 and Attachment 2 section 6 and the VSLs be consistent. The Technical Rational document, page 6, par. 3 states “The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems.” Request that the “their low impact BES Asset(s) and/or” be struck. The inclusion of these words brings non-BCS into scope.	
Likes 0	
Dislikes 0	
Response	
Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren would like more clarification on what is considered malicious activity. In Attachment 1 Section 6, Ameren believes that 6.2 and 6.3 should be switched because the determination to disable the vendor's access would be made after suspicious communication has been detected.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo

Answer	
Document Name	

Comment

Suggest to restrict to scope of section 6.3 to Asset contacting a Low Impact BCS at a control center or remove the section 6.3 sub requirement entirely. The rationale is the low impact BCS should not have a higher requirement that medium impact. Alternatively, include the detection of known/suspected inbound and outbound malicous communication requirement in Medium Impact BCS that is not control center, since the justification of using Intermediate system and multifactor authentication (CIP-005 IRA requirements) as a risk mitigation does not cover system to system communciations from/to vendors.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	
Document Name	

Comment

Once again, we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.

Request consistency the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.”

Recommend consistency between Attachment 1, Section 6 and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one of more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:”

Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The

equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for medium impact that is not at a Control Center.

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “One or more method(s) for detecting known or suspected inbound and outbound malicious communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	

Comment

Once again, we requested a redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.

Request consistency in the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.”

Recommend consistency between Attachment 1, Section 6, and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one or more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:”

Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact

BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for the medium impact that is not at a Control Center.

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “One or more method(s) for detecting known or suspected inbound and outbound malicious communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2, and 6.3.

Likes 0	
Dislikes 0	

Response

Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light

Answer	
Document Name	

Comment

Seattle City Light abstains

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	
Document Name	

Comment

See comments as supplied by Deanna Carlson from Cowlitz PUD.

Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5	
Answer	
Document Name	
Comment	
There should be additional clarification on Attachment 1 Section 6.3. It appears that Low Requirement has a larger scope than the corresponding Medium Requirement. As written, Section 6.3 applies to all vendor communications.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2020-03 Supply Chain Low Impact Revisions | Draft 3
Comment Period Start Date:	7/6/2022
Comment Period End Date:	8/19/2022
Associated Ballot(s):	2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 3 ST

There were 75 sets of responses, including comments from approximately 175 different people from approximately 105 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Summary Response

Low impact BES Cyber Systems

The SDT would like to centrally address the concept of "Low having more requirements than Medium at Control Centers", and particularly Attachment 1 Requirement 6.3. While the SDT can agree that CIP-005 R1.5 applies only at High and Medium Control Centers, the issue facing the SDT was the requirement of the SAR and the risk that it exposes. Currently, there are 23 standards that apply to Low only, that number is less than half of those that apply to Medium. This was purposeful because of their Low risk. However, when one considers the data compiled

by NERC only 11% of High and Medium assets have IP connectivity, while the number for Low is 58% and when you consider those entities with Low only that number jumps to 66%. While Low's have a low risk profile, the number of those assets connected with IP routable connections is more than five times that of High and Medium, while, High and Medium have more than twice the requirements. While adding a requirement to monitor malicious vendor traffic might look on the surface as "extending more requirements to Low than Medium", it is not the case, considering the risk profile of the connections into those assets. Additionally, the largest difference between CIP-005 R1.5 and CIP-003 Attachment 1 Section 6 is that Section 6 is relevant only to vendor electronic remote access, where CIP-005 is relevant to all communications.

Desire for "active" and "session" to be added to language

The Standard Drafting Team has had significant discussions over the last three postings on the use of the term "active." In the first two postings, the team used in the context of the Board Directive, but in the third posting the SDT decided to remove the term based on commenters concerns of unintended consequences. The team further discussed that the use of the term could create an administrative burden regarding the implied audit requirement to document when, and how, active vendor sessions occur. The team attempted to address the issue by updating the language in Section 6 so that the statement "as established under Section 3.1" applies to all parts of Section 6 to better define the communications scope. This provides the ability for entities to have more flexibility to address the scope of the requirements. The SDT did not want to limit compliance activities to a 'session'. The SDT believes that entities should determine whether a session-based approach is warranted for the risk presented to their entity.

Desire for updated or new definitions

The SDT would like to address comments around definitions in a single response. In general, the SAR for this team does not allow for new and/or modified definitions, however, there are additional reasons why this team did not add, modify, or use inappropriate definitions. Terms like Interactive Remote Access or IRA are inappropriate for use in CIP-003 because the use of this term would require technology or requirements to be use that are not applicable for low impact BES Cyber Systems, for example IRA requires an Electronic Security Perimeter or ESP that is not required at lows today (see NERC Glossary of Terms Glossary_of_Terms.pdf (nerc.com))

Adding new definitions was also a concern for the SDT, however as mentioned about the SAR did not allow the addition, but more importantly, the SDT had to consider what the addition of new terms might have on other standards. As an example, consider "vendor", which is already used in an approved standard. Adding a definition such as this would have far reaching issues with already enforceable standards, thus the team declined to create definitions for this reason.

Attachment 1 Section 6.3 not clearly scoped to vendor communications only

The SDT thanks you for your comment. The SDT has made no substantive clarifying changes to address this concern.

Questions

1. Do you agree the updated languge proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The team has added clarifying languge to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT has added clarifying language that limits the scope to Section 3.1. Do you believe the language in Attachement 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT is proposing a 36-month implementation plan for Attachment 1, Section 6 based on industry feedback. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section

6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

7. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Carnesi	Chris Carnesi		WECC	NCPA	Marty Hostler	Northern California	4	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Agency		
					Dennis Sismaet	Northern California Power Agency	6	WECC
Santee Cooper	James Poston	3		Santee Cooper	Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Susan Sosbe	Wabash Valley Power Association	3	RF
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Ryan Strom	Buckeye Power, Inc.	5	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Colette Caudill	East Kentucky Power Cooperative	1,3	SERC
					Michael Brytowski	Great River Energy	3	MRO
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
LaKenya VanNorman	LaKenya VanNorman		SERC	Florida Municipal Power Agency (FMPA)	Chris Gowder	Florida Municipal Power Agency	5	SERC
					Dan O'Hagan	Florida Municipal Power Agency	4	SERC
					Carl Turner	Florida Municipal Power Agency	3	SERC
					Jade Bulitta	Florida Municipal	6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Agency		
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Power Company		
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Paul Haase	Paul Haase		WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Harish Vijay Kumar	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Tim Kelley	Tim Kelley		WECC	SMUD / BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal	6	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Utility District		
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree the updated languge proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The introduction of "detecting known or suspected malicious communications" for low impact BES Cyber Systems would be more stringent as compared to CIP-005 R1.5 since Medium Impact BES Cyber Systems are not applicable in the current version of the standards without adding any additional reliability benefits.	
Likes 4	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre; WEC Energy Group, Inc., 3, Kane Christine; Central Hudson Gas & Electric Corp., 1, Ridolfino Michael; Jones Barry On Behalf of: sean erickson, Western Area Power Administration, 1, 6;
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

As with the previous draft, Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS (i.e., those outside of control centers). Section 6.3 would require detection of malicious inbound and outbound communications for low impact BCS with vendor remote connectivity. In the current version and next effective version of CIP-005, Part 1.5 requires detection of malicious inbound and outbound communications only for medium impact BCS at Control Centers.

BPA recognizes that the NERC Board Resolution directs the drafting team to modify CIP-003 to "..include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications…" BPA also acknowledges that the Technical Rationale attempts to identify more robust controls from CIP-005-6 that offset this inconsistency. However, this inconsistency results in a complicated and confusing compliance approach: entities will be required to develop separate evidence packages for Low and Medium (outside of control centers) substations even if they implement identical solutions across both.

Likes 4	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre; Platte River Power Authority, 6, Martz Sabrina; Platte River Power Authority, 3, Kiess Wade; Wabash Valley Power Association, 3, Sosbe Susan
Dislikes 0	

Response

The SDT thanks you for your comment. The SDT understands your comment that having a difference between low (CIP-003-X) language and high/medium (CIP-005) language will create more and varied evidence for submission. The SDT agrees that this is possible, and is a necessary result due to the large number of entities with low-impact BES Cyber systems

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the opportunity to comment and thanks the drafting team for their continued efforts.

The language proposed in CIP-003-X attachment 1 Section 6 does not comprehensively address the risk of malicious communication and vendor remote access to low impact BES cyber systems with possible areas of improvement as follows:

- The language used in CIP-003-X attachment 1 Section 6.3 is referring to 'known or suspected malicious communications'. BC Hydro recommends adding more clarity and provide examples of use cases and applicability. Specifcally, context and usage of the term 'malicious communication' needs more clarity and BC Hydro requests to provide the context and usage with pertinent examples and use case scenarios to improve understanding and to better scope the requirements.
- Similarly, BC Hydro proposes defining and adding term 'Vendor Electronic Remote Access' to NERC Glossary of Terms.
- Who and what is considered a 'Vendor' also need to be defined in the Glossary of Terms for clarity and understanding.

CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote acces's however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5.

BC Hydro recommends rewording or removing Section 6.3 completely.

Likes 1	Jones Barry On Behalf of: sean erickson, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

The SDT thanks you for your comment.
1st bullet: The drafting team specifically left open the definitions and specifics of terms that are not already in the NERC glossary. This should enable entities to define those risks internally and manage them appropriately

2nd and 3rd Bullet: One entity asked the SDT to add "Vendor Electronic Access" to the NERC glossary. The SDT decided that the follow-on effects of such an addition (ie: how would this affect other, existing NERC standards) is not within the scope of this SAR, nor is it beneficial to the security of the BES if NERC codifies such a definition.

Many entities commented that the draft language sets a higher standard of security for Low impact BES Cyber systems, than is set by CIP-005-7 which is only applicable to medium and high impact systems. The SDT respectfully disagrees. CIP-005-7 mandates many things including:

- documentation of EAPs -specific inbound and outbound permissions, -deny by default -Dial-up authentication -malicious detection of all connections, not just from vendors. None of the previous list is explicitly required by the SDT's or current language of CIP-003-X	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Attachment 1 Section 6 was introduced as an objective risk-based requirement; however, it lists prescriptive actions. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection. As such the language should read more like an objective risk-based requirement allowing an entity to have a bit more leeway to comply with the requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT had a SAR that specifically required protection from vendors, and that inserting more protections would increase compliance cost dramatically.Attachment 1, Section six subsections are in line with the NERC Board resolution requirements outlined in the Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security SAR. Outside of requiring that entities develop and implement processes to mitigate common risks associated with vendor remote access (as outlined in the December 2019 NERC Supply Chain Risk Assessment report) the standard allows entities to determine the most appropriate method(s) to meet compliance. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

Tacoma Power does not agree that the proposed language in Attachment 1, Section 6 addresses the risk of malicious communication. The Section 6 introduction includes an objective risk-based high-level requirement, yet prescriptive actions are listed in the sub-parts. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection.

Tacoma Power suggests the following wording to avoid prescriptive language in the sub-parts (changes noted in italics and important word changes are highlighted with bold text):

Section 6**:** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall ***address*****:**

6.1 determining and disabling ***active*** *vendor electronic remote access sessions,* ***if applicable****; and*

6.2 malicious communications.

By altering the wording as shown above, an entity would be able to comply through multiple means and would not HAVE to implement a detection method to mitigate malicious communication. For example, if an Entity makes use of an Intermediate System for all low impact BCS remote access, which would mitigate the risk of vendor electronic remote access malicious communications, they have addressed malicious communications without having to also detect malicious communications, which in this scenario is extremely unlikely to occur.

Likes 3	Platte River Power Authority, 6, Martz Sabrina; Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response	
Thank you for your comment. The SDT feels that the current language is the best version that allows entities maximum flexibility for program design and follow-through.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE continues to be concerned that the language in Attachment 1, Section 6 is limited to vendor remote access. Texas RE is concerned that Section 6's focus on vendor remote access does not capture the full range of malicious communications contemplated under the low impact guidance documents. In the event of a supply chain attack, malicious communications can occur whether or not a Responsible Entity has established an authorized channel for vendor communications. Additionally, in the event of a supply chain attack, malicious communications can potentially be initiated from compromised Cyber Assets attempting to communicate with a Command and Control server. Importantly, these can occur along logical pathways for which where the Responsible Entity has deliberately not established channels for vendor remote access. A supply chain attack, such as the supply chain attack that resulted in the 2020 United States federal government data breach, is not typically conducted directly by compromised vendors themselves. These attacks are typically conducted by malicious third parties that do not have a formal business relationship with the vendor or the affected Registered Entity. As such, scoping this requirement to only address remote access that is conducted directly by vendors would deliberately exclude from scope the exact communications that need to be monitored. Based on this perspective, therefore, Texas RE recommends that the SDT clarify that CIP-003 low impact monitoring obligations extend to all inbound and outbound network traffic to mitigate the risk of suspicious or malicious traffic going unnoticed, not just in situations of authorized vendor remote access. Texas RE recommends moving the proposed language in Attachment 1, Section 6.2 to Section 3 (Electronic Access Controls) so it is clear malicious communication monitoring and detection method obligations apply to all communications, not simply vendor remote access communications.	
Likes 0	

Dislikes 0	

Response
Thank you for your comment. The SDT agrees that our language does not capture all possible malicious situations at low impact BES Cyber Systems. We see this as outside the scope of our given SAR. Our SAR also instructed the SDT to write language for vendor threats. Given the nature (larger sample size, lower grid risk) we feel that the draft language is appropriate. The SDT believes that the security controls are comminserate with the risks for low impact.

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Since Section 6 has introduced an objective risk-based high-level requirement, yet prescriptive actions are listed. An entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT had a SAR that specifically required protection from vendors, and that inserting more protections would increase compliance cost dramatically.Attachment 1, Section six subsections are in line with the NERC Board resolution requirements outlined in the Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security SAR. Outside of requiring that entities develop and implement processes to mitigate common risks associated with vendor remote access (as outlined in the December 2019 NERC Supply Chain Risk Assessment report) the standard allows entities to determine the most appropriate method(s) to meet compliance. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	
Comment	

Reclamation recommends the SDT align the CIP-003 Attachment 1 Section 6 language with CIP-005-6 R2 and use NERC-defined terms where possible. The content of Section 6 should be included within Attachment 1 Section 3 and not made into a new section. Reclamation recommends adding “if technically feasible” to Section 6.2 to account for leagacy systems that are not capable of detecting known or suspected malicious communications for both inbound and outbound communications.

Reclamation recommends the following changes to Section 6:

From:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor remote access (including interactive and system-to-system access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for determining vendor remote access sessions;

6.2 Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and

6.3 Having one or more method(s) for disabling vendor remote access.

To:

Vendor remote access: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) to low impact BES Cyber Systems that includes:

6.1 Having one or more method(s) for identifying active vendor remote access sessions;

6.2 If technically feasible, have one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications; and **6.3** Having one or more method(s) for disabling active vendor remote access. The phrase “determining active vendor remote access sessions” is not clear. Reclamation recommends using the same language as in the Technical Rationale, which refers more specifically to ”when sessions are initiated.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT feels that the current language is the best version that allows entities maximum flexibility for program design and follow-through.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC support Tacoma Power's comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Tacoma Power.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	No
Document Name	
Comment	
Section 6.3 still creates a higher bar for some assets containing low impact BCS than for most medium impact BCS (i.e., those outside of control centers). It is still not clear is VPN connections established with support vendors fully adheres to requirement or additional steps such as IDS/IPS are required. The Section 6 introduction includes an objective risk-based high-level requirement, yet prescriptive actions are listed in the sub-parts.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. A few entities mentioned VPNs (virtual private networks) and IDS/IPS (intrusion detection/prevention systems). The SDT does not see a difference between vendor remote communications over VPN vs non-VPN - we think that protections need to be in place in either scenario. An IDS/IPS may be used by an entity as part of its compliance program (note that IDS/IPS is listed as only one of the examples in Attachment 2 Section 6) but would require (as would any other device or system) a program that included statements and actions that would satisfy the mandates of Sections 6.1, .2 and .3. To expand on the example - if an entity wanted to use an IDS/IPS for CIP-003-X compliance, the applicable program would need to include how the system would disable vendor remote access when required (to satisfy section 6.2). The SDT had a SAR that specifically required protection from vendors, and that inserting more protections would increase compliance cost dramatically.Attachment 1, Section six subsections are in line with the NERC Board resolution requirements outlined in the Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security SAR. Outside of requiring that entities develop and implement processes to mitigate common risks associated with vendor remote access (as outlined in the December 2019 NERC Supply Chain Risk Assessment report) the standard allows entities to determine the most appropriate method(s) to meet compliance. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
NCPA does not agree with prescriptive language for 6.3 as it relates to detect known or suspected malicious communications. This would be more arduous for Low impact entities to implement compared to non-Control Center Medium Impact facilities as they don't need to comply with CIP-005 R1.5. This creates an imbalance of requiring lower risk facilities to comply with a more strenuous requirement than higher risk facilities. At least limiting 6.3's scope to only Low Impact Control Centers would be somewhat congruent with the CIP-005 R1.5 requirement.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, please see responses to comments below.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
Malicious communication can arguably be effectively addressed with Attachment 1, requirements 6.1 and 6.2. We believe that Requirement 6.3 is excessive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT feels that the current language is the best version that allows entities maximum flexibility for program design and follow-through.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
It is not clear that Section 6.3 only applies to only inbound and outbound vendor communication and not all communication established under Section 3.1. If Section 6.3 is applicable to all communications then it should be moved to Section 3.1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. We see your comment that the latest draft language now includes non-vendors in the requirements of Section 6.3. The SDT respectfully disagrees - Section 6.3 is under the text of Section 6, which specifically asks entities to "mitigate risks associated with vendor remote access....". It was not the intent of the SDT to include non-vendor access in section 6.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Based on comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see response on your comments below.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Based on the comments below, we conclude the proposed updates do not adequately address the risk of malicious communication and vendor remote access.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. Please see response on your comments below.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Deanna Carlson.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD does not agree that the proposed language in Attachment 1, Section 6 addresses the risk of active malicious communications and is too prescriptive in the actions listed in Section 6.1 – 6.3. Entities can mitigate the risks associated with vendor electronic remote access through various means and still address the NERC Board Resolution to detect, determine, and disable active vendor electric remote access, and malicious communications. The language should read more like an objective risk-based requirement allowing an entity to have a bit more leeway to comply with the requirement. Additionally, as written Section 6.3 appears to be applicable to all communications and should then be removed from Section 6.3 and placed in Section 3.1 if this was the intent.	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT had a SAR that specifically required protection from vendors, and that inserting more protections would increase compliance cost dramatically. Attachment 1, Section six subsections are in line with the NERC Board resolution requirements outlined in the Revisions to CIP-003-8 for Low Impact BES Cyber Systems for Supply Chain Cyber Security SAR. Outside of requiring that entities develop and implement processes to mitigate common risks associated with vendor remote access (as outlined in the December 2019 NERC Supply Chain Risk Assessment report) the standard allows entities to determine the most appropriate method(s) to meet compliance. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.

Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment, please see response to EEI And MRO NSRF.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the proposed language in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impace BES cyber systems as directed by the NERC Board resolution.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the updated language in Attachment 1, Section 6 addresses the risks noted by the NERC Board of Trustees resolution.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI agrees that the updated language proposed in Draft 3 of Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see response to EEI.	
Kimberly Turco - Constellation – 6	
Answer	Yes
Document Name	
Comment	
Yes, Constellation agrees the the updated language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comments.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Yes, Constellation agrees the the updated language addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comments.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While the language added to the standard does meet the NERC Board resolution, we still strongly disagree with adding malicious code detections for low impact BCS (specifically Section 6.3) as this control is not a requirement for medium impact BCS (not at Control Centers). Although these new requirements come from the FERC/NERC resolution, there are much greater risks to the overall BES/BPS, at medium impact BCS than low impact BCS. We feel the only resolution to this, is to add the same controls to medium impact BCS or drop the requirement for low impact. If we as an ERO are taking a risk based approach and the FERC/NERC resolution into consideration, then adding the requirement to medium impact BCS is the only possible resolution to satisfy us and the FERC/NERC resolution. Based on our research there is not a resolution to add malicious code detections to medium impact BCS and therefore we will not be in favor of the controls for low impact.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment please see summary response.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the updated language proposed in Draft 3 of Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2020-03_Supply_Chain_Lows_Unofficial_Comment_Form (GSOC FINAL).docx
Comment	
GSOC believes the updated language in section 6 addresses the risk; however modifications to section 6.3 introduce confusion regarding the scope of the requirement over the last posting by arguably including non-vendor related communications in the language. This broadening of language could be read to include asset-level monitoring of all inbound and outbound communication for known or suspected malicious communications is a significant departure from the previous draft and would result in an unduly burdensome compliance mandate. The Technical Rationale developed by the SDT states that section 6.3 "is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report." However, the SDT has removed the language from 6.3 that clarifies this scope. Since the SDT moved the language that states "where such access has been established under Section 3.1" to the main part of Section 6, this language could be read as requiring this detection to occur at the point where access is established under Section 3.1 which defines that access at each asset containing low impact assets. Further, 6.3 could be read to require all malicious	

communications to be detected, regardless of whether it is vendor communication or not as there is no reference to vendor communication in the control specified in section 6.3.

GSOC respectfully proposes the following wording that reverts the language in 6.3 to the language of the prior posting:

Vendor Electronic Remote Access Security Controls: For assets containing

low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible

Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.

These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote

access;

6.2 One or more method(s) for disabling vendor electronic remote

access; and

6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT sees that your comment in the latest draft language now includes non-vendors in the requirements of Section 6.3. The SDT respectfully disagrees - Section 6.3 is under the text of Section 6, which specifically asks entities to "mitigate risks associated with vendor remote access....". It was not the intent of the SDT to include non-vendor access in section 6.

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rob Watson - Choctaw Generation Limited Partnership, LLLP - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	

Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

***2. The team has added clarifying languge to limit the scope of this access to remote access that is conducted by vendors. Do you believe that this language is clear? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification*.**	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Cowlitz PUD would like to see the terms 'vendor electronic remote access'; added to Section 6.3 as it is included in Section 6.1 and 6.2. By excluding this from Section 6.3 an interpretation could be applied to malicious communications more broadly than as was intended.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the team has made this clarifying change.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	

Response	
Please see response to Deanna Carlson	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
The CIP Standards use many terms: Vendor electronic remote access (proposed CIP-003) Inbound and outbound electronic access (CIP-003, Section 3) User-initiated interactive access (CIP-003 Reference Model 5) Indirect access (CIP-003 Reference Models 6 and 9) Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the summary response regarding definitions.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

The CIP Standards use many terms such as: Vendor electronic remote access (proposed CIP-003), Inbound and outbound electronic access (CIP-003, Section 3), User-initiated interactive access (CIP-003 Reference Model 5), Indirect access (CIP-003 Reference Models 6 and 9). Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see the summary response regarding definitions.

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
GSOC believes the updated language in section 6, specifically section 6.3 does not clarify the scope of the requirement. The language that provided that clear scoping was removed in this posting. Section 6.3 could now be read to require all malicious communications to be detected, regardless of whether it is vendor communication or not as there is no reference to vendor communication in the control specified in section 6.3. GSOC respectfully proposes the following wording which reverts the language in 6.3 to that of the prior posting: Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associatedwith vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access; 6.2 One or more method(s) for disabling vendor electronic remote access; and 6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren believes the term vendor needs to be more defined more clearly. Does the vendor role make a difference (contractor operators, support, etc.)? Is operations different from support in terms of vendors?	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	

Answer	No
Document Name	
Comment	

The second paragraph of Attachment 1 states “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s).” It is unclear how this statement can be applied without clarification on how the terms used in CIP-005-7 relate to the proposed terms in CIP-003-x. Request clarification on how the CIP-003-X term “vendor electronic remote access” relates to the CIP-005-7 terms “active vendor remote access” (R2) and “vendor-initiated remote connections”(R3).

The CIP Standards use many terms:

· Vendor electronic remote access (proposed CIP-003)

· Inbound and outbound electronic access (CIP-003, Section 3)

· User-initiated interactive access (CIP-003 Reference Model 5)

· Indirect access (CIP-003 Reference Models 6 and 9)

Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?

Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, please see summary response.

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	No
Document Name	

Comment	
Please define if “Vendor Electronic Remote Access” is only for Interactive Access or does it include system to system access as well.	
Likes 0	
Dislikes 0	
Response	
The team believes vendor electronic remote access is all access conducted by a vendor.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
The CIP Standards use many terms: {C}· Vendor electronic remote access (proposed CIP-003) {C}· Inbound and outbound electronic access (CIP-003, Section 3) {C}· User-initiated interactive access (CIP-003 Reference Model 5) {C}· Indirect access (CIP-003 Reference Models 6 and 9) Suggest using an existing term OR request clarification of the “vendor electronic remote access” term - what is the purpose of electronic? What is remote?	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see the summary response regarding definitions.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC support Tacoma Power's comment.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends adding “Vendor” to the NERC Glossary of Terms and proposes the following definition: Vendor - Persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts to supply equipment for BES Cyber Systems and related services. Vendor does not include other NERC-registered entities that provide reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). Vendor may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
While the high-level Section 6 introduction includes scoping language, the wording of the sub-parts 6.1 & 6.2 include the same vendor electronic remote access language, while 6.3 does not. Sub-part 6.3 may be construed to apply more broadly due to the omission of the scoping language in this sub-part, because the other sub-parts include this scoping language. PGS recommends including the language "vendor remote access".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	No
Document Name	
Comment	
Sections 6.1 and 6.2 use the terms 'vendor electronic remote access'; however, Section 6.3 does not use this language which could lead to confusion for utilities. Even though the high level Section 6 limits the scope to remote access conducted by vendors, Section 6.3, without	

having the same language as Sections 6.1 and 6.2, could be interpreted to apply to malicious communications more broadly and not just for vendor electronic remote access. Suggested language: In Section 6.3, instead of saying "One or more method(s) for detecting known or suspected inbound and outbound malicious communications," the suggested language is as follows: "One or more method(s) for addressing and mitigating known or suspected inbound and outbound malicious communications for vendor electronic remote access"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
While the high-level Section 6 introduction includes scoping language, the wording of the sub-parts 6.1 and 6.2 include the same vendor electronic remote access language, while 6.3 does not. Sub-part 6.3 may be construed to apply more broadly due to the omission of the scoping language in this sub-part, because the other sub-parts include this scoping language. Tacoma Power recommends including the "vendor remote access" language to the sub-part 6.3 sentence, in accordance with the the following Westlaw reference: https://content.next.westlaw.com/practical-law/document/Ibe943df6e1e711e698dc8b09b4f043e0/Expressio-unius-est-exclusio-alterius?viewType=FullText&transitionType=Default&contextData=(sc.Default)&firstPage=true	
Likes 2	Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	

Response	
Thank you for your comment. The team has made clarifying changes to the language.	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The term “vendor” needs to be defined in the NERC glossary of terms. The use of the term “vendor” in the CIP-013 Supplemental Material is not an official definition. This term is crucial to CIP-013 and with the proposed changes to CIP-003 the term will be crucial in determining what is considered vendor remote access.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
As mentioned in comments related to Question 1 above, 'vendor electronic remote access' needs clarity of understanding and clear definitions of the terms for appropriate applicability as well as the use of term 'Vendor' e.g., whether a consultant using same infrastructure is considered vendor.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see summary response.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
We appreciate the time and attention the SDT put forth working on this section, however we are concerned that the language under 6.3 does not include a direct reference to “vendor remote accesss” in the sub part. We understand the SDT debated this issue, however we recommend modification to the language to improve clarity. We believe these clarifications can be made without substantial change, so are thereby voting affirmative with the desire for futher clarification. These are possible improvements to the language: 1) Adding clarity to the last sentence of section 6:	

"These vendor electronic remote access processes shall include:" By adding "vendor electronic remote access", it helps clarify the intent of all three sub-sections being applicable to just "vendor electronic remote access" and not all communications. While technically the word "these" refers to the previous sentence, we feel there could be more calrity to assist Responsisble Entities to focus on the subject of the revisions. 2) Remove references to “vendor remote access” in 6.1 and 6.2 3) Modifying 6.3 to include a reference to vendor electronic remote access. If 6.3 were modified, we recommend it to read: “6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications associated with vendor electronic remote access.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	

Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI supports the Draft 3 language believing that it is sufficiently clear to limit the scope for remote access to low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
We appreciate the time and attention the SDT put forth working on this section, however we are concerned that the language under 6.3 does not include a direct reference to “vendor remote accesss” in the sub part. We understand the SDT debated this issue, however we recommend modification to the language to improve clarity. We believe these clarifications can be made without substantial change, so are thereby voting affirmative with the desire for futher clarification. These are possible improvements to the language: 1) Adding clarity to the last sentence of section 6: "These vendor remote access processes shall include:" By adding "vendor remote access", it helps clarify the intent of all three sub-sections being applicable to just "vendor remote access" and not all communications. While technically the word "these" refers to the previous sentence, we feel there could be more calrity to assist Responsisble Entities to focus on the subject of the revisions. 2) Remove references to “vendor remote access” in 6.1 and 6.2 3) Modifying 6.3 to include a reference to vendor remote access. If 6.3 were modified, we recommend it to read: “6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications associated with vendor remote access.”	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see response to EEI.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
I believe the language is clear however the level of monitoring is not reduced.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #2.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	

Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Yes, Constellation believes that the language is clear. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Yes, Constellation believes that the language is clear. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	

Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI supports the Draft 3 language believing that it is sufficiently clear to limit the scope for remote access to low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the language is clear that remote access is only for vendors.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
I believe the language is clear however the level of monitoring is not reduced.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern believes the language added is clear to limit the scop of remote access conducted by vendors.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI and MRO NSRF.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	

Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank youf for your comment.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
The technical rationale explains that Section 6.3 is specific to vendor only communication. It would aid the reader's understanding if this is clarified in the actual CIP-003-X standard language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

As noted in its response to Question 1 above, Texas RE continues to believe that the low-impact standards being developed should not be limited solely to vendor communications. However, if the SDT elects to limit the focus of these requirements solely to vendor communications, Texas RE notes that because the SAR specifically states that CIP-003-8 should be revised to include policies for low impact BES Cyber Systems at locations that allow vendor remote access, Texas RE recommends including "at locations that allow vendor remote access" in Section 6 as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made clarifying changes to the language.	

***3. Has the SDT clarified that Attachment 1 Section 6 only addresses vendor's access to low impact assets containing BES cyber systems from remote locations? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification*.**

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The use of word "Remote" will need some clarification and perhaps a definition in the defined terms, e.g., how the "Remote" term will be used in the sample scenarios below: 1) On site, but electronically remote (i.e. has to go through EAP despite being at the station). 2) A "vendor" at the work location of Responsible Entity, also electronically remote (i.e. going through EAP). 3) "Traditionally" remote, off site, and electronically remote (also going through EAP).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	No
Document Name	
Comment	

The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	No
Document Name	
Comment	
The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Micah Runner - Black Hills Corporation - 1,3,5,6	

Answer	No
Document Name	
Comment	
The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	No
Document Name	
Comment	
The language says “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Access from remote locations is not the same as remote access. A vendor could be physically on site and connect to the system through a remote connection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT discussed on-prem and off-prem vendors and their methods of access and took this into consideration. In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3. Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team considered specific language regarding vendor, electronic, remote, access, etc.., as well as comments and suggestions from other entities. Please see our general comments regarding the Section 3 and Section 6, which is applicable to vendor remote access, which should clarify the discussion of requirements language choices. The SDT determined to focus on language which allows entities to define and determine their specific process(es) for vendor remote access.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC believes the updated language in section 6, specifically section 6.3 does not specifically limit the scope of the requirement to vendor access and communications. GSOC respectfully proposes the following wording:

Vendor Electronic Remote Access Security Controls: For assets containing

low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible

Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.

These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote

access;

6.2 One or more method(s) for disabling vendor electronic remote

access; and 6.3 One or more method(s) for detecting known or suspected malicious communications for both inbound and outbound vendor communications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Request clarification on why Attachement 1, 6.3 does not use the phrase "vendor electronic remote access" while Section 6 and, 6.1 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3. Request confirmation that the SDE expects all of Attachement 1, Section 3.1 to be in place before Section 6 requirements. If section 3.1 is not met, then Section 6 does not apply.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team considered specific language regarding vendor, electronic, remote, access, etc.., as well as comments and suggestions from other entities. Please see our general comments regarding the Section 3 and Section 6,	

which is applicable to vendor remote access, which should clarify the discussion of requirements language choices. The SDT determined to focus on language which allows entities to define and determine their specific process(es) for vendor remote access.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2, and 6.3. Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. Please see the summary comments regarding language. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Deanna Carlson.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
The language says, “electronic remote access” it does not state “remote locations,” which is appropriate based on the guidance given for CIP-005, which made it clear that “remote access” may include access originating from a desk in your corporate office. The geographic location of the vendor shouldn’t matter, only the method used to access the BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The standard drafting team has taken these comments into consideration and In an effort to develop requirements which meet a vast array of organizations, technologies, processes and operations, the SDT chose language which allows entities to identify and develop a process(es) regarding when and how vendors achieve access.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

The language in Section 6, 'where such access has been established under Section 3.1' implies the entity is not required to implement a process to 'mitigate risks associated with vendor electronic remote access' unless remote access has been (or will be) established. We believe this is appropriate, where entities have opted to categorically deny all electronic remote access to vendors.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI and MRO NSRF.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

The language is clear for Section 6.1 and 6.2 that it clarifies this section is specific for Vendor Electronic Remote Access. Section 6.3 could be somewhat ambiguous and may be read to include more than vendor remote access.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications to Attachment 1, Section 6 and those modifications clearly indicate it is for vendor access from a remote location.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

The wording in sub-parts 6.1 & 6.2 include the same “vendor electronic remote access” language, while subpart 6.3 does not. Sub-part 6.3 should read the same as sub-parts 6.1 & 6.2 so as not to imply that 6.3 should be more broadly enforced beyond its intended purpose.	
Likes 1	Wike Jennie On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merre
Dislikes 0	
Response	
Thank you for your comment, the SDT has updated the language in 6.3 to clarify the intent.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI’s comment: EEI agrees that Attachment 1, Section 6 clarifies that vendor’s access to low impact assets containing BES cyber systems is limited to remote locations.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Yes. The SDT clarified that Attachment 1 Section 6 only applies to vendor access to low impact assets containing BES cyber systems from remote (off-site) locations. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Yes. The SDT clarified that Attachment 1 Section 6 only applies to vendor access to low impact assets containing BES cyber systems from remote (off-site) locations. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
See comments under question 2 to help clarify this.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that Attachment 1, Section 6 clarifies that vendor's access to low impact assets containing BES cyber systems is limited to remote locations.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, please see response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	

Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

***4. The SDT has added clarifying language that limits the scope to Section 3.1. Do you believe the language in Attachement 1 Section 6 limits the scope to low impact BES cyber systems? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification*.**	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Additional clarification needs to ensure that the scope of Section 6 applies only to low impact BES Cyber Systems where vendors are actually given remote access. The language as written can be interpreted that all low impact BES Cyber System that are identified in Section 3.1 should have a process in place to detect, determine, and disable active vendor electric remote access, and malicious communications, regardless of vendors having remote access or not.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. You are correct the standard was written so that every asset containing low impact BES Cyber Systems where vendor electronic remote access is allowed and the communications conditions outlined in Section 3.1 are subject to the requirements of Section 6. In Section 3.1 the statement "Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are..." combined with the statement in Section 6 ": For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1." are the statements which cover whether you must apply Section 6. If you do not allow vendor electronic remote access and the conditions of Section 3.1 are not met, then Section 6 does not apply.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	
Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply. Request clarification on how Sections 3.1 and 6 impact the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT does intend that all of the conditions of Attachment 1, Section 3.1 be met as a pre-condition for Section 6. Attachemtn 1 is included in the VSL for Requirement R2.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Request confirmation that the SDT expects all of Attachement 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply. Request clarification on how Sections 3.1 and 6 impacts the VSLs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT does intend that all of the conditions of Attachment 1, Section 3.1 be met as a pre-condition for Section 6. Attachemtn 1 is included in the VSL for Requirement R2.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	

Answer	No
Document Name	
Comment	
Request confirmation that the SDT expects all of Attachment 1, Section 3.1 to be in place before Section 6 requirements. If Section 3.1 is not met, then Section 6 does not apply. Request clarification on how Sections 3.1 and 6 impact the VSLs	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. CIP-003 R2 idneitifeds all requirements for BES Cyber Systems to meet the security requirements laid out in Attachment 1. The SDT does intend that all of the conditions of Attachment 1, Section 3.1 be met as a pre-condition for Section 6. Attachemtn 1 is included in the VSL for Requirement R2.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
NCPA does not agree with prescriptive language for 6.3 as it relates to detect known or suspected malicious communications. This would be more arduous for Low impact entities to implement compared to non-Control Center Medium Impact facilities as they don't need to comply with CIP-005 R1.5. This creates an imbalance of requiring lower risk facilities to comply with a more strenuous requirement than higher risk facilities. At least limiting 6.3's scope to only Low Impact Control Centers would be somewhat congruent with the CIP-005 R1.5 requirement.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. Why and how the Requirement in Section 6.3 applies to 'Low Impact BCS' is not very clear from the language used. The Section 6.3 does offer possible mitigation of the risks i.e., 'malicious communication and vendor remote access' however this is even more stringent on Low Impact BCS in comparison to CIP-005-5 R1.5. BC Hydro recommends rewording or removing Section 6.3 completely.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

There is confusion with the language used in Section 6 as to whether it pertains to the assets containing the low impact BES Cyber Systems (which may contain out of scope cyber systems) or the low impact BES Cyber Systems themselves.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the summary response.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, please see response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed language in Section 6 limits that scope to Section 3.1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
The proposed changes to limit scope are redundant. Section 3.1 and Section 6 are explicit to low impact BCS. If vendor remote access wasn't already established and allowed under Section 3.1, there would either be a violation of Section 3.1 or a CIP exceptional circumstance would need to be declared. The language is fine, but unnecessary to try to confine the scope of Section 6 as it is very explicit to low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #4.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI agrees that the proposed language in Section 6 limits that scope to Section 3.1.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the modification to Section 3.1 make it clear the scope of the Requirement is for low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI and MRO NSRF.	
Russell Noble - Cowlitz County PUD - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Benjamin Winslett - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	
Thank you for your support.	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

5. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The scope should be narrowed to just where the risk exists as opposed to a broad swath of assets. The way it is written it implies that all communications need to be monitored to determine malicious communications through vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has made changes to the language in section 6.3 to clarify the intent.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Although the cost may differ between entities, BC Hydro's assessment is that the impact may change based on understanding & clarity of terms and scope of application. As advised in comments of Question 1 above, CIP-005-5 R1.5 does not apply to Medium impact BCS if they are not at Control Centers. However requirement in CIP-003-X Section 6.3 applies to 'Low Impact BCS' which is even more stringent	

on Low Impact BCS in comparison to CIP-005-5 R1.5, where only High and Medium Impact BCS at Control Centers are in scope leaving all the other Medium impact BCS out of scope. Implementing this requirement and adding detection methods for known or suspected malicious communications for both inbound and outbound communications concerning Low impact BCS will likely have significant cost impact.

Likes 0	
Dislikes 0	

Response
Thank you for your comment, please see summary response.
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment
Including a more restrictive prescriptive control for malicious communication detection for low impact BCS that does not exist for medium impact BCS not at a Control Center is not a cost-effective approach. Medium impact BCS not at a Control Center must still follow CIP-005 R2 for remote access through an intermediate system. This was mentioned as justification for including Section 6.3 for low impact but not requiring for Medium impact BCS not at a Control Center. If an entity implements CIP-005 R2 Intermediate Systems for low impact, they will still not be compliant with CIP-003, Attachment 1, Section 6.3 as currently worded. In order to provide a more cost effective solution, Tacoma Power suggests that an entity can mitigate the risks associated with vendor electronic remote access through various means and still address disabling of vendor electric remote access, and malicious communication protection. Suggested wording to avoid prescriptive language and provide a more cost effective solution:

Section 6**:** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall ***address*****:** *6.1 determining and disabling* ***active*** *vendor electronic remote access sessions,* ***if applicable****; and* *6.2 malicious communications.*	
Likes 2	Platte River Power Authority, 3, Kiess Wade; Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	
Thank you for your comment. The team has added language to section 6 to clarify this intent. Additionaly, see summary response above.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	No
Document Name	
Comment	
Section 6.3 is written in prescriptive way toward only one of many possible solutions for addressing malicious communications. This does not allow entities to analyze and choose the most cost effective approach to addressing and mitigating malicious communication.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT feels that the current language is the best version that allows entities maximum flexibility for program design and follow-through.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Including a more restrictive prescriptive control for malicious communication detection for low impact BCS that does not exist for medium impact BCS not at a Control Center is not a cost-effective approach. Medium impact BCS not at a Control Center must still follow CIP-005 R2 for remote access through an intermediate system. This was mentioned as justification for including Section 6.3 for low impact but not requiring for Medium impact BCS not at a Control Center. If an entity implements CIP-005 R2 Intermediate Systems for low impact, they will still not be compliant with CIP-003, Attachment 1, Section 6.3 as currently worded.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation identifies that it is not cost effective to have separate standards for low impact and medium impact BES Cyber Systems, especially when the language of the requirements for each impact level is identical. Reclamation observes that Project 2016-02 will bring many changes to a majority of the CIP standards; therefore, Reclamation recommends Project 2016-02 is a good avenue to incorporate low impact requirements into the CIP standards and avoid the continuous churn of CIP-003 Attachment 1 when ultimately the requirements for low impact BES Cyber Systems will end up being identical to those for medium impact BCS.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT maintains that entities with only low-impact assets, are subject to CIP-003 only and this is why medium and low impact are in separate standards. This team has coordinated with Project 2016-02 and is attempting to minimize the number of versions of CIP-003 that become enforceable.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC support Tacoma Power's comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Tacoma Power.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
We do not have enough information at this time to address cost-effectiveness of the revisions.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
Cost effectiveness of Attachment 1, 6.1, 6.2, and 6.3 is unknown at this time since the capability will require a technical solution not currently in place. Further, this requirement is not consistent with current CIP-005-6 and future CIP-005-7 enforceable requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT maintains that entities with only low-impact assets, are subject to CIP-003 only and this is why medium and low impact are in separate standards.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
There is a high probability that new technology controls will be required to meet the new requirements. Entities would need to allocate funds and projects to implement new technologies.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
There is a high probability that new technology controls will be required to meet the new requirements. Entities would need to allocate funds and projects to implement new technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Russell Noble - Cowlitz County PUD - 3	

Answer	No
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
Thank you for your commnet, please see response to Deanna Carlson.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
The scope should be modified to read more like an objective-based requirement allowing entities more leeway and potentially more cost-effective means to comply with the specific list of assets identified. Recognition that not all communications need to be monitored to determine malicious communications through active vendor remote access will ensure resources are focused on actual risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT feels that the current language is the best version that allows entities maximum flexibility for program design and follow-through.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Xcel Energy agrees that the modifications can be implemented in a cost-effective manner when implemented within the timeframe identified in the associated Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
Until an approved Standard is in place, PG&E cannot make a determination if the modification are cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

It is cost effective, but these costs will be pushed directly to ratepayers which requires FERC support to answer the ratepayers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
We requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, redline to last approved it posted with final ballot.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI’s comments.	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST abstains.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	

Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	

We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	
Document Name	
Comment	
NextEra Energy is not supplying a position nor comment on cost effectiveness of these changes.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation will not comment on cost. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation will not comment on cost.	

Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
Unable to justify cost effectiveness at this time	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost-effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	

Answer	
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
Once again, we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, redline to last approved is provided during final ballot.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	

Comment	
Once again, we requested a redline to the last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances of approval. Otherwise, TFIST abstains from commenting on cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, redline to last approved is provided during final ballot.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

6. The SDT is proposing a 36-month implementation plan for Attachment 1, Section 6 based on industry feedback. Would these proposed timeframes give enough time to put into place process, procedures or technology to meet the proposed language in Section 6? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	No
Document Name	
Comment	
It is difficult to estimate as the scope of 6.3 is not clear yet.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The team has made changes to 6.3 to clarify intent.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
While WECC does not believe the extended 36-month Implementation Plan is reason to vote NO, we believe that considering the risks that are facing the system, the DT should consider moving the Implementation back to 24 months as was included in earlier versions of the draft standard. However, if a 36-month Implementation Plan is what is necessary to gain approval of the Standard, WECC understands.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team extended the timeline based on feedback from industry in the previous two ballots and believes this timeframe is the most appropriate.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro recommends a longer implementation plan, e.g. more than ~36 months, considering the cost and scope impact as identified in comments to Question 1 and 4 above. Once the clarity of terms and definitions is obtained as identified in comments to Question 1 and 4, BC Hydro will be in a better position to provide an alternate detailed implementation plan to meet the target completion deadline.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team decided on a 36 month timeline based on feedback from industry in the previous two ballots and believes this timeframe is the most appropriate.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Large entities with hundreds of low impact facilities will need more implementation time for addressing the changes applicable to low impact assets. Suggested timeline is a 5 year plan, implementing 20% of the assets per year.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team decided on a 36 month timeline based on feedback from industry in the previous two ballots and believes this timeframe is the most appropriate.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD, Segment 5 8/19/2022	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree with 36 months. Request deletion of the following language because this language refers to a removed Section – “Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the team has removed the identified language from the implementation plan.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Agree with 36-months. Request deletion of the following language because this language refers to a removed Section - "Where the standard drafting team identified the need for a longer implementation period for compliance with a particualar section of a proposed Reliability Standard (i.e., and entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard does into effect at an earlier date."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the team has removed the identified language from the implementation plan.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the EEI response	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed 36-month implantation plan for attachment 1, Section 6.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power is in agreement with EEI's comments.	
Likes 0	
Dislikes 0	
Response	

The SDT thanks you for your comment, please see response to EEI.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy thanks the Standard Drafting Team for this important revision. We fully support the proposed implementation timeline.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the SDT’s proposed implementation timeframe recommendation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes

Document Name	
Comment	
We agree with 36-months. Request deletion of the following language because this language refers to a removed Section – "Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the team has removed the identified language from the implementation plan.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Increasing the implementation time from 18 to 36 months should allow adequate time for implementation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Risk: Supply chain risk to be taken into factor.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Alan Kloster - Alan Kloster On Behalf of: Jennifer Flandermeyer, Evergy, 3, 6, 5, 1; Jeremy Harris, Evergy, 3, 6, 5, 1; Kevin Frick, Evergy, 3, 6, 5, 1; Marcus Moor, Evergy, 3, 6, 5, 1; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #6.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	

Comment	
Yes. The proposed 36 months would give enough time to put the process, procedures and technology in place to meet the proposed language in Section 6. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Yes. The proposed 36 months would give enough time to put the process, procedures and technology in place to meet the proposed language in Section 6. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes

Document Name	
Comment	
NextEra Energy supports EEI's comment: EEI supports the proposed 36-month implantation plan for attachment 1, Section 6.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the 36-month implementation plan and that it would be sufficient time for PG&E to implement the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Increasing the implementation time from 18 to 36 months should allow adequate time for implementation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and supports the proposed 36-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see response to EEI and MRS NSRF.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the 36 calendar month implementation.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaKenya VanNorman - LaKenya VanNorman On Behalf of: Chris Gowder, Florida Municipal Power Agency, 5, 3, 4, 6; Richard Montgomery, Florida Municipal Power Agency, 5, 3, 4, 6; - LaKenya VanNorman, Group Name Florida Municipal Power Agency (FMPA)	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Devon Tremont - Taunton Municipal Lighting Plant - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Caulson - Megan Caulson On Behalf of: Jennifer Wright, Sempra - San Diego Gas and Electric, 5, 3, 1; - Megan Caulson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michelle Amarantos - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Public Utility District No. 1 of Snohomish County, 1, Rhoads Alyssia
Dislikes 0	
Response	
Thank you for your support.	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Eric Sutlief - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	
Comment	

Seattle City Light abstains	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
We do not have insight to whether this is cost effective or not so Black Hills Corporation will not be providing a comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

***7. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired*.**	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes redline versions of-proposed Standards should be markups to "last approved," not markups to previous proposed versions. The practice of redlining previous drafts makes it difficult to compare proposed new or modified requirement language to current, in-effect requirements. NST believes the SDT should, in addition to addressing the NERC Board resolution, revise CIP-003 Requirement R2 to state that documented cyber security plan(s) for a Responsible Entity's low impact BES Cyber Systems are required to address Attachment 1 Sections 3, 5, and 6 only if the following conditions exist: For Section 3, only if one or more of the Responsible Entity's assets that contain low impact BCS has external connectivity of a type that matches the descriptions in Sections 3.1 and/or 3.2. For Section 5, only if TCAs and RMs are used at one or more of the Responsible Entity's assets that contain low impact BCS and are occasionally connected to BCS. For Section 6, only if (a) Section 3.1 is applicable and (b) vendor remote access is permitted. A Responsible Entity with no vendor remote access should not be expected to document how it addresses Section 6 requirements.	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT posts redline to last approved on the final ballot. Please see SDT summary response re. the alignment of the standard revisions with the approved SAR. Section 6 requires Responsible Entities to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. An acceptable process of mitigation may be for an entity to completely restrict such access; in this case, an entity may want to document associated controls or policies associated with these restrictions.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	
Document Name	
Comment	
We appreciate the time and level of effort that the Drafting Team has put in to address the many concerns related to vendor access to Low Impact Cyber Systems. Their efforts will eventually result in modifications to CIP-003 that will benefit the industry, protect the Bulk Electric System, and better serve the ratepayers.	
Likes 0	
Dislikes 0	

Response
The SDT thanks you for your comment.

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE recommends the following revisions be made to the CIP-003-X Technical Rationale document for clarity:

1. Define the acronym “SAR” as “Standard Authorization Request” and

2. On page 5, under “1. Electronic remote access:”, add a statement to clarify that “electronic remote access” includes interactive and system-to-system remote access.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT has revised the Technical Rationale document to ensure the full name for 'Standard Authorization Request' is used in the first instance of its use, with the commonly understood acronym 'SAR' used thereafter.

Per the Techncial Rationale, the SDT avoided using NERC defined terms: Interactive Remote Access in order to prevent applying high and medium impact requirements upon low impact assets and systems

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

Attachment 1, Section 6, sub-section 3. The wording is good but can further be clarified by adding “for vendor electronic remote access” to the end:

One or more method(s) for detecting known or suspected inbound and outbound malicious communications **for vendor electronic remote access**.

Attachment 2, Section 6, sub-section 3. (examples of evidence) the wording is good but can further be clarified:

Network based Anti-malware technologies such as deep packet inspection;

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS); or Automated or manual log reviews; or Automated User Behaviour Analytics (UBA); or SIEM network traffic or vendor remote access log analysis and alerting; or other operational, procedural, or technical controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In light of industry feedback, and for absolute clarity, the SDT has revised 6.3 to add 'for vendor electronic remote access'. The SDT notes that this was the original intent of section 6.3 as it was anticipated that the vendor remote access criteria from the Section 6 'parent' statement applied to all the sections (6.1-6.3) below. At this time the SDT will not be adding additional evidence examples. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.	
Joe Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of EEI and the MRO NSRF.	
Likes 0	
Dislikes 0	

Response	
The SDT thanks you for your comment, please see response to EEI and MRO NSRF.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	
Document Name	
Comment	
In the Consideration of Comments document for the Draft 2 ballot, the SDT states that "…the SDT believes "remote access" is any access that crosses this boundary (Attachment 1 Section 3.1). If a vendor is "onsite" but starts the connection process outside this boundary, this connection should be considered remote access." CHPD believes that by including this statement in the Technical Rational document it will provide stakeholders and the ERO Enterprise with a better understanding of the requirements in the CIP-003-X Reliability Standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. As outlined in CIP-003-X, Attachment 1, Section 6, the scope of CIP-003-X Section 6 is limited by the access condition outlined in Section 3.1 of Attachment 1. The SDT agrees with the statement "If a vendor is "onsite" but starts the connection process outside this boundary, this connection should be considered remote access."	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Consider updating Section 6.3 to be more clear in identifying the language is specifically geared towards Vendor Electronic Remote Access **only**.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. In light of industry feedback, and for absolute clarity, the SDT has revised 6.3 to add 'for vendor electronic remote access'. The SDT notes that this was the original intent of section 6.3 as it was anticipated that the vendor remote access criteria from the Section 6 'parent' statement applied to all the sections (6.1-6.3) below.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	
Document Name	
Comment	
BC Hydro ackowledges the SDT's effort and hard work which went into putting together these complex changes to CIP-003-X. As identified in comments of question 1 to 4 above, the definitions of terms and clarity of application with some specific industry use case examples will help providing a more clear understanding and likely result in a faster and appropriate approvals of these proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see SDT responses to questions above.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	

PG&E wishes to thank the SDT for listening to the industry's input and the effort in making these modifications to address the NERC Boards resolution	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Claudine Bates - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Sheila Suurmeier - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Micah Runner - Black Hills Corporation - 1,3,5,6	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ron Wilgers - Black Hills Corporation - 3 - WECC	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	
Document Name	
Comment	
NextEra Energy thanks the SDT for its service of improving the security of the bulk electric system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation does not have any additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation does not have additional comments. Kimberly Turco on behalf of Constellation Segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; - MEAG Power - 1 - SERC	
Answer	
Document Name	
Comment	
Even though Attachment 1, Section 6 addresses the risk of malicious communication, it does so in a prescriptive way in that the standard is directing utilities toward a particular solution (e.g. detecting with software/hardware or detection processes) rather than allowing the utility to choose the best approach/method to address and mitigate malicious communication.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT summary comments regarding the draft standards alignment with the final SAR.	

The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
In Attachment 1, Section 6, Texas RE recommends specifying “pursuant to CIP-002” rather than referencing another NERC Reliability Standard, as requirements should be complete and self-contained as noted in the Ten Benchmarks of an Excellent Reliability Standard. Texas RE recommends the following language: “For each asset that contains a low impact BES Cyber System, and for which the Responsible Entity allows vendor remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access.” Additionally, Texas RE recommends the SDT Include language for (1) software integrity and authenticity, (2) information system planning, and (3) vendor risk and procurement controls, which addresses various aspects of supply chain risk management as is consistent with Reliability Standards CIP-013 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT will not be adopting Texas RE's suggested language as the cross-referencing of standards is consistent within CIP-003 and the SDT would like to remain consistent with this approach. Thank you for the additional recommended controls, please see the SDT summary comments re. aligning the draft standard with the approved SAR.	
JT Kuehne - AEP - 6	
Answer	
Document Name	

Comment	
No additional comments at this time. AEP thanks the SDT for their efforts on this draft.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has noted the recommendation.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
BHE requests the words "and timeframes [keep the "to"] authorize," be removed from the Technical Rationale, page 5: "The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access." BHE is concerned this reference to timeframes and authorization could lead Regional Entities to question both, when neither appear in the 6.1 obligation to determine access. BHE also recommends for Attachment 2, Section 6.3, to lowercase "Intrusion Detection System/Intrusion Prevention System" since it's not a glossary term and not a formal name. Thanks to the SDT for the fine work on this standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

The Technical Rationale is intended to help industry to understand the technology and technical elements in the Reliability Standard. The SDT would like to emphasize that Regional Entities are required to assess compliance based on the language of the Reliability Standard and the facts and circumstances presented. Though not NERC defined terms, Intrusion Detection System and Intrusion Prevention System (and associated acronyms) are commonly used and understood in their capitalized form. For this reason, the SDT will not be editing them to be lowercase at this time.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
With the consideration of the FERC NOPR. Additional architecture diagrams should be illustrated for a possible IDS/IPS implementation similar to when EAC under section 3, there was guidance architecture diagrams.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT is unable to consider FERC NOPRs in comment stage. The SDT encourages entities to engage with FERC directly on this NOPR F via appropraite stakeholder consultation opportunities.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
None. Thank you for the opportunity to comment.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for your comment.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
Is the intent of this section to not include dial-up? If so, it would be better to clarify in the language.	
Likes 0	
Dislikes 0	
Response	
Thank you for comment. The scope of CIP-003-X Section 6 is limited by the access condition outlined in Section 3.1 of Attachment 1. Based on this scope limitation dial-up is not included.	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval. Request consistency the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each	

require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.”

Recommend consistency between Attachment 1, Section 6 and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one of more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:”

Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for medium impact that is not at a Control Center.

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “One or more method(s) for detecting known or suspected inbound and outbound malicious communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers.

Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT posts redline to last approved on the final ballot. Additionally, please see the SDT response to Utility Services, Inc. and the SDT summary responses which address your additional concerns.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	
Comment	
The NAGF requests the SDT to consider adding language in Attachment 2 Section 6.3 to clarify that documentation of vendor contractual agreements to maintain malicious communication security controls would be an appropriate approach to meet compliance with Attachment 1 Section 6.3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Per Chapter 3 of the NERC ERO Enterprise Registration Procedure, A registered entity may delegate the performance of a task to another entity, including a non-registered party, using a third-party agreement. However, the registered entity may not delegate its responsibility for ensuring the task is completed. In all cases, NERC and the REs will hold the registered entity accountable for compliance responsibilities and violations thereof. Third-party written agreements are determined on a case-by-case basis between the registered entity and the third-party NERC Compliance is the responsibility of the Registered Entity and cannot be outsourced to a third-party vendor.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Like NAGF, Duke Energy asks the Standard Drafting Team to consider adding language in Attachment 2 Section 6 Part 3 to explicity clarify that documentation of vendor contractual agreements to maintain malicious communication security controls could be an approach to comply with Attachment 1 Section 6.3. Without this addition, compliance with the revisions could be challenging for OEM connections, given that many vendors consider their communications with covered equipment to be proprierty information or intellectual property that they are not willing to have inspected.	

We also recommend that the Drafting Team reconsider the one example in Attachment 2 Section 6 Part 3 where it says “anti-malware technologies e.g. full packet inspection.” We would either like to see the one example taken away, or more added, since one example could imply one best option.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Per Chapter 3 of the NERC ERO Enterprise Registration Procedure, A registered entity may delegate the performance of a task to another entity, including a non-registered party, using a third-party agreement. However, the registered entity may not delegate its responsibility for ensuring the task is completed. In all cases, NERC and the REs will hold the registered entity accountable for compliance responsibilities and violations thereof. Third-party written agreements are determined on a case-by-case basis between the registered entity and the third-party NERC Compliance is the responsibility of the Registered Entity and cannot be outsourced to a third-party vendor. The SDT encourages entities to review Chapter 3 of the NERC ERO Enterprise Registration Procedure and work with vendors to update commercial agreements such that the entity is able to procure the required evidence to fulfil their compliance requirements. The SDT has included a revised implementation plan of 36 months, in part to accommodate for these potential commercial contract complexities. The example of 'full packet inspection' has been removed. The SDT would like to reinforce the message that the examples included in Attachment 2 are not intended to dictate appropriate compliance evidence nor are they intended to limit an entity in determining what evidence they provide.	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their efforts and allowing the industry to participate in the drafting process	

Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Section 6 states “the Responsible Entity shall implement a process“while CIP-003-X R2, for which Section 6 is dependent, requires the implementation of a plan. The second paragraph in Attachment 1 states “Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s).” Additionally, Attachment 2, Section 6 states “For Section 6.3, documentation showing implementation of processes or technologies”. The VSL related to Section 6 only references a “plan”. Suggest removing the requirement to use a “process” from Attachment 1 section 6. Additionally, suggest that the language of Attachment 1 Section 6 and Attachment 2 section 6 and the VSLs be consistent. The Technical Rational document, page 6, par. 3 states “The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems.” Request that the “their low impact BES Asset(s) and/or” be struck. The inclusion of these words brings non-BCS into scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT use of the word 'process' in Attachment 1 Section 6 reflects the requirement to document and implement a set of required instructions specific to the Responsible Entity and to achieve the specified outcomes in Section 6.1 thru 6.3. These processes should be documented as part of the overall CIP-003-X R2 requirement to implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems.	

Per the background provided in the currently approved CIP-003-7 standard, the term process does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements. The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. The SDT appreciates that the VSL related to R2 Attachment 1, Section 6 and has updated the term from 'plan' to 'processes' Consistent with the rest of CIP-003, the SDT has revised the wording in the technical rationale to only refer to BES Cyber Systems.	
Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren would like more clarification on what is considered malicious activity. In Attachment 1 Section 6, Ameren believes that 6.2 and 6.3 should be switched because the determination to disable the vendor's access would be made after suspicious communication has been detected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes that the term malicious activity is a common used and understood industry term. The SDT feels that the provision of case studies or examples of malicious activity would quickly become outdated. The SDT encourages entities to utilize other more current sources of information to remain current on the ever-evolving threat landscape. Examples include, but are not limited to: E-ISAC, CISA, ERO Reliability Risk Priorities Report, NERC Low Impact White Paper (currently in draft). The order of the CIP-003-X Section 6 requirements does not reflect the order in which entities may be required to perform these tasks. It is possible that an entity may disable vendor electronic remote access in absence of a detection of suspected inbound and/or outbound malicious communications.	

Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	
Document Name	
Comment	
Suggest to restrict to scope of section 6.3 to Asset contacting a Low Impact BCS at a control center or remove the section 6.3 sub requirement entirely. The rationale is the low impact BCS should not have a higher requirement that medium impact. Alternatively, include the detection of known/suspected inbound and outbound malicous communication requirement in Medium Impact BCS that is not control center, since the justification of using Intermediate system and multifactor authentication (CIP-005 IRA requirements) as a risk mitigation does not cover system to system communciations from/to vendors.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the SDT summary response related to this concern.	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	

Once again, we requested redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval.

Request consistency the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.”

Recommend consistency between Attachment 1, Section 6 and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one of more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:”

Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for medium impact that is not at a Control Center.

Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “One or more method(s) for detecting known or suspected inbound and

outbound malicious communications." 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6's Applicable Systems says "Medium impact BCS at Control Centers" 6.3 applies to all vendor communications, not just Control Centers. Request clarification on why Attachment 1, 6.3 does not use the phrase "vendor electronic remote access" while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2 and 6.3.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The SDT posts redline to last approved on the final ballot. The SDT use of the word 'process' in Attachment 1 Section 6 reflects the requirement to document and implement a set of required instructions specific to the Responsible Entity and to achieve the specified outcomes in Section 6.1 thru 6.3. These processes should be documented as part of the overall CIP-003-X R2 requirement to implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems. Per the background provided in the currently approved CIP-003-7 standard, the term process does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements. The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. Please see SDT summary comments that address the concern that low impact controls outlined in CIP-003-X Section 6.3 are higher than high and medium impact controls required in CIP-005

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	

Once again, we requested a redline to last approved. SMEs need to see red lines to the currently effective standard, to adequately review the proposed changes. Without this red line, the review is very challenging and may reduce the chances for approval. Request consistency in the Attachment 1 Section 6 terms. The current language requires a plan, a process, processes, and methods but evaluates compliance based on security controls. 1) CIP-003 R2 states ”shall implement one or more documented cyber security plan(s)”; 2) Attachment 1 Section 6 first says “shall implement a process“ and then says “These processes shall include”; 3) Section 6.1 – 6.3 each require “One or more methods”; and 4) The VSL for R2 states: “but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6.” Recommend consistency between Attachment 1, Section 6, and other Attachment 1 Sections by changing “process” to “plan.” Suggest changing from “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a process to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:” to “For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one or more plans to mitigate risks associated with electronic vendor electronic remote access, where such access has been established under Section 3.1. These plans shall include:” Request clarification on how a new Low Impact Requirement can be a higher bar than the corresponding High / Medium Impact Requirements. The equivalent requirement to Section 6.3, for high and medium impact, is CIP-005-7 R1.5 which is only applicable to high impact BCS and medium impact BCS at a Control Center. The existing 6.3 would require a low impact control that is not required for the medium impact that is not at a Control Center. Request clarification on Attachment 1 Section 6.3. Why a Low Requirement has a larger scope than the corresponding Medium Requirement (CIP-005 R1.6) The proposed Requirement for CIP-005 R1.6 says “detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.” 6.3 says “One or more method(s) for detecting known or suspected inbound and outbound malicious communications.” 6.3 applies to all vendor communications, not just IP. Next CIP-005 R1.6’s Applicable Systems says “Medium impact BCS at Control Centers” 6.3 applies to all vendor communications, not just Control Centers. Request clarification on why Attachment 1, 6.3 does not use the phrase “vendor electronic remote access” while Section 6 and, 6.1 and 6.2 use this phrase. While in the parent language, we request consistency among 6.1, 6.2, and 6.3.	
Likes 0	

Dislikes 0	

Response
Thank you for your comment. The SDT posts redline to last approved on the final ballot. The SDT use of the word 'process' in Attachment 1 Section 6 reflects the requirement to document and implement a set of required instructions specific to the Responsible Entity and to achieve the specified outcomes in Section 6.1 thru 6.3. These processes should be documented as part of the overall CIP-003-X R2 requirement to implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems. Per the background provided in the currently approved CIP-003-7 standard, the term process does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements. The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. The SDT appreciates that the VSL related to R2 Attachment 1, Section 6 and has updated the term from 'plan' to 'processes' Please see SDT summary comments that address the concern that low impact controls outlined in CIP-003-X Section 6.3 are higher than high and medium impact controls required in CIP-005

Paul Haase - Paul Haase On Behalf of: Hao Li, Seattle City Light, 4, 5, 3, 6, 1; - Paul Haase, Group Name Seattle City Light	
Answer	
Document Name	

Comment
Seattle City Light abstains

Likes 0	
Dislikes 0	

Response

The SDT thanks you for your comment.	
Russell Noble - Cowlitz County PUD - 3	
Answer	
Document Name	
Comment	
See comments as supplied by Deanna Carlson from Cowlitz PUD.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	
Document Name	
Comment	
There should be additional clarification on Attachment 1 Section 6.3. It appears that Low Requirement has a larger scope than the corresponding Medium Requirement. As written, Section 6.3 applies to all vendor communications.	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see summary response.	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	

Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
The SDT thanks you for your comment, please see response to EEI.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2020-03 Supply Chain Low Impact Revisions | CIP-003-X

Additional Ballot and Non-binding Poll Open through August 19, 2022

Now Available

The additional ballot for **CIP-003-X - Cyber Security — Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Friday, August 19, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Balloting
Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions
CIP-003-X

Formal Comment Period Open through August 19, 2022

Now Available

A 45-day formal comment period for reliability standard **CIP-003-X - Cyber Security — Security Management Controls**, is open through **8 p.m. Eastern, Friday, August 19, 2022**.

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) are both making modifications to CIP-003. The Supply Chain team is using "-X" in place of the version number, and Virtualization used "-Y". The version number will be assigned upon adoption by the NERC Board of Trustees.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 10-19, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2020-03 Supply Chain Low Impact Revisions” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/253)
Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X AB 3 ST
Voting Start Date: 8/10/2022 12:01:00 AM
Voting End Date: 8/19/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 248
Total Ballot Pool: 291
Quorum: 85.22
Quorum Established Date: 8/19/2022 1:48:23 PM
Weighted Segment Value: 66.81

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	78	1	48	0.727	18	0.273	0	2	10
Segment: 2	6	0.1	1	0.1	0	0	0	3	2
Segment: 3	69	1	40	0.667	20	0.333	0	3	6
Segment: 4	20	1	8	0.5	8	0.5	0	1	3
Segment: 5	64	1	35	0.686	16	0.314	0	2	11
Segment: 6	47	1	25	0.694	11	0.306	0	2	9
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	1	0	0	0	0	0	0	0	1
Segment: 10	5	0.4	3	0.3	1	0.1	0	1	0
Totals:	291	5.5	160	3.675	74	1.825	0	14	43

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Mike Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	Seattle City Light	Michael Jang		None	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Taunton Municipal Lighting Plant	Devon Tremont		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	None	N/A
1	Wind Energy Transmission Texas, LLC	doug whitworth		None	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Independent Electricity System Operator	Harishkumar Subramani Vijay Kumar		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Brendan Baszkiewicz		Abstain	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Negative	Third-Party Comments
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	Wabash Valley Power Association	Susan Sosbe		Negative	Third-Party Comments
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	American Public Power Association	John McCaffrey		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	DTE Energy	patricia ireland		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Christopher Siewert		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		None	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young	Helen Zhao	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Marty Watson		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright	Megan Caulson	None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		None	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Negative	Third-Party Comments
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 1 of Pend Oreille County	April Owen		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Pam Syrjala		Negative	Comments Submitted
6	Santee Cooper	Glenda Horne		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		None	N/A
9	British Columbia Utilities Commission	Sarosh Muncherji		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 291 of 291 entries

BALLOT RESULTS

Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X | Non-binding Poll AB 3 NB
Voting Start Date: 8/10/2022 12:01:00 AM
Voting End Date: 8/19/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 233
Total Ballot Pool: 277
Quorum: 84.12
Quorum Established Date: 8/19/2022 1:56:23 PM
Weighted Segment Value: 67.84

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	74	1	39	0.709	16	0.291	8	11
Segment: 2	6	0.1	1	0.1	0	0	3	2
Segment: 3	68	1	35	0.66	18	0.34	8	7
Segment: 4	19	1	8	0.5	8	0.5	0	3
Segment: 5	60	1	29	0.69	13	0.31	7	11
Segment: 6	44	1	20	0.69	9	0.31	6	9
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	1	0	0	0	0	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	5	0.3	3	0.3	0	0	2	0
Totals:	277	5.4	135	3.65	64	1.75	34	44

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Comments Submitted
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Mike Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Great River Energy	Gordon Pietsch		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		None	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		None	N/A
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Taunton Municipal Lighting Plant	Devon Tremont		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	None	N/A
1	Wind Energy Transmission Texas, LLC	doug whitworth		None	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Independent Electricity System Operator	Harishkumar Subramani Vijay Kumar		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Brendan Baszkiewicz		Abstain	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand	John Daho	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	Wabash Valley Power Association	Susan Sosbe		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	American Public Power Association	John McCaffrey		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	DTE Energy	patricia ireland		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Comments Submitted
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	None	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Christopher Siewert		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		None	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Marty Watson		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright	Megan Caulson	None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		None	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Pam Syrjala		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Santee Cooper	Glenda Horne		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
9	British Columbia Utilities Commission	Sarosh Muncherji		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the standard, posted for a 10-day ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 18, 2020
SAR posted for comment	April 8, 2020
45-day formal comment period with ballot	August 27 – October 11, 2021
45-day formal additional comment period with ballot	February 25 – April 15, 2022
45-day second additional formal comment period with ballot	July 6 – August 19, 2022

Anticipated Actions	Date
10-day final ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-9:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-9.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic	remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Version	Date	Action	Change Tracking
9	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third final 4510-day formal comment period with ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 18, 2020
SAR posted for comment	April 8, 2020
45-day formal comment period with ballot	August 27 – October 11, 2021
45-day formal additional comment period with ballot	February 25 – April 15, 2022
45-day second additional formal comment period with ballot	July 6 – August 19, 2022

Anticipated Actions	Date
10-day final ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-X9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~X~~9:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-9X.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1)	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber	of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by	topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to	containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media	implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2,	Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security ~~plan(s)~~process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2,	Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security ~~plan(s)~~process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security ~~plan(s)~~process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-X9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days of the change. (R4)	calendar days of the change. (R4)	calendar days of the change. (R4)	title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Version	Date	Action	Change Tracking
X9	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS,

router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;

- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies ~~(e.g., full packet inspection technologies)~~;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the standard, posted for a 10-day ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 18, 2020
SAR posted for comment	April 8, 2020
45-day formal comment period with ballot	August 27 – October 11, 2021
45-day formal additional comment period with ballot	February 25 – April 15, 2022
45-day second additional formal comment period with ballot	July 6 – August 19, 2022

Anticipated Actions	Date
10-day final ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~8~~9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

~~All BES Facilities.~~

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~8~~9:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-9.

~~See Implementation Plan for CIP-003-8.~~

~~**6. Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation;~~ and~~

1.2.6. Vendor electronic remote access security controls; and

~~**1.2.6.**~~**1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

~~1.1.~~ Compliance Enforcement Authority:

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~1.3.~~ Evidence Retention:

~~1.4.~~1.2. The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

~~**1.5. Compliance Monitoring and Assessment Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~**1.6. Additional Compliance Information:**~~

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems, but did not address one of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address two of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address three of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	four or more of the ~~six~~seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	the previous approval. (R1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or	Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic	remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~8~~9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Version	Date	Action	Change Tracking
9	TBD	Revisions to address NERC Board Resolution and the Supply Chain Report	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy

appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Vendor Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents

- ~~Appropriate notifications upon discovery of an incident~~
- ~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

- ~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~
- ~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~
- ~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

- ~~Process(es) to declare a CIP Exceptional Circumstance~~
- ~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~Requirement R2:~~

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a

combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Section 6. Monitoring as a physical security control can be used as a complement or an alternative to physical access control.: Examples of monitoring controlsevidence showing the implementation of the process for Section 6 may include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, For Section **3 – Electronic Access Controls**

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing

low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the

~~specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

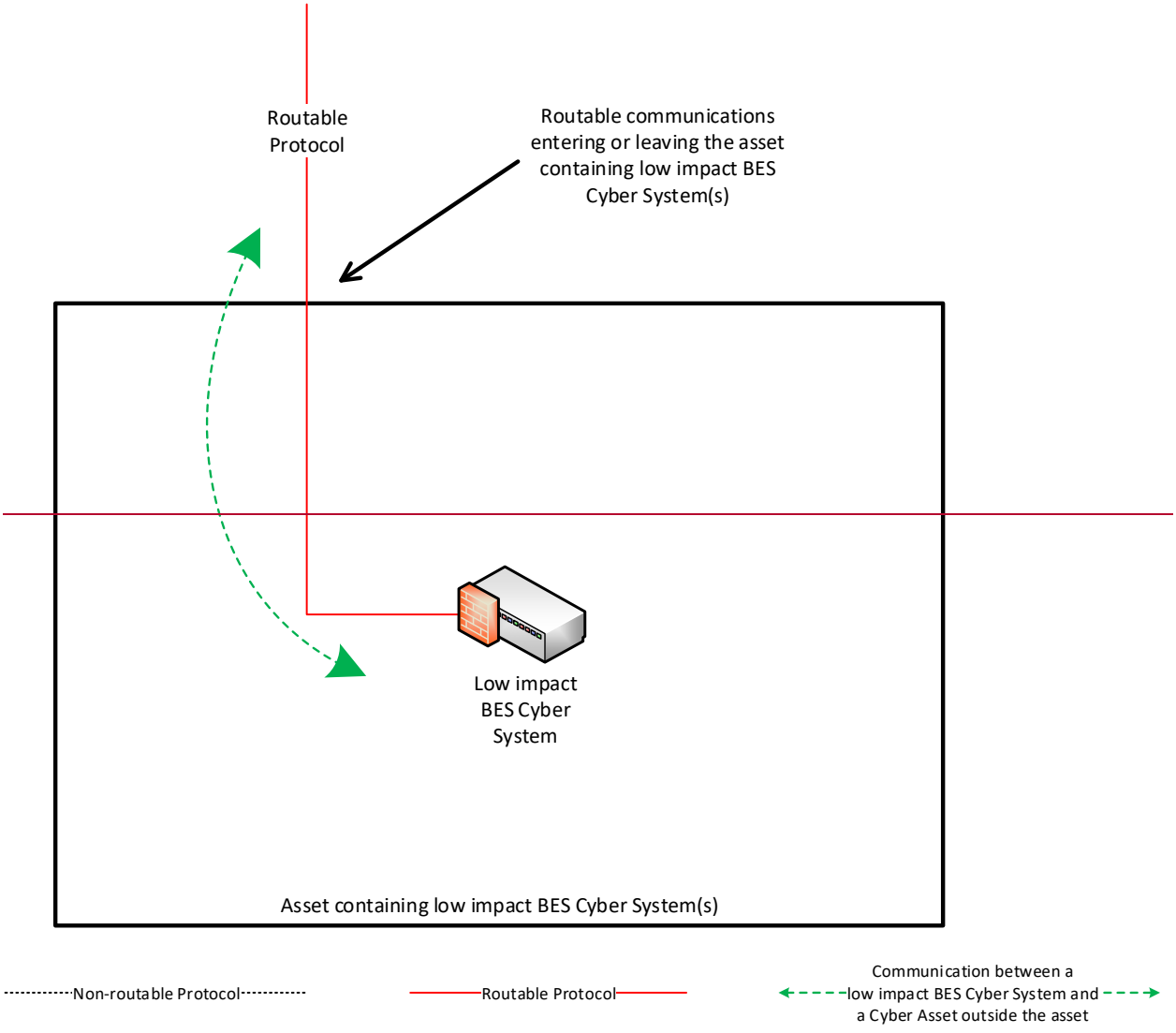
~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

~~**NOTE:**~~

- ~~This is not an exhaustive list of applicable concepts.~~
- ~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

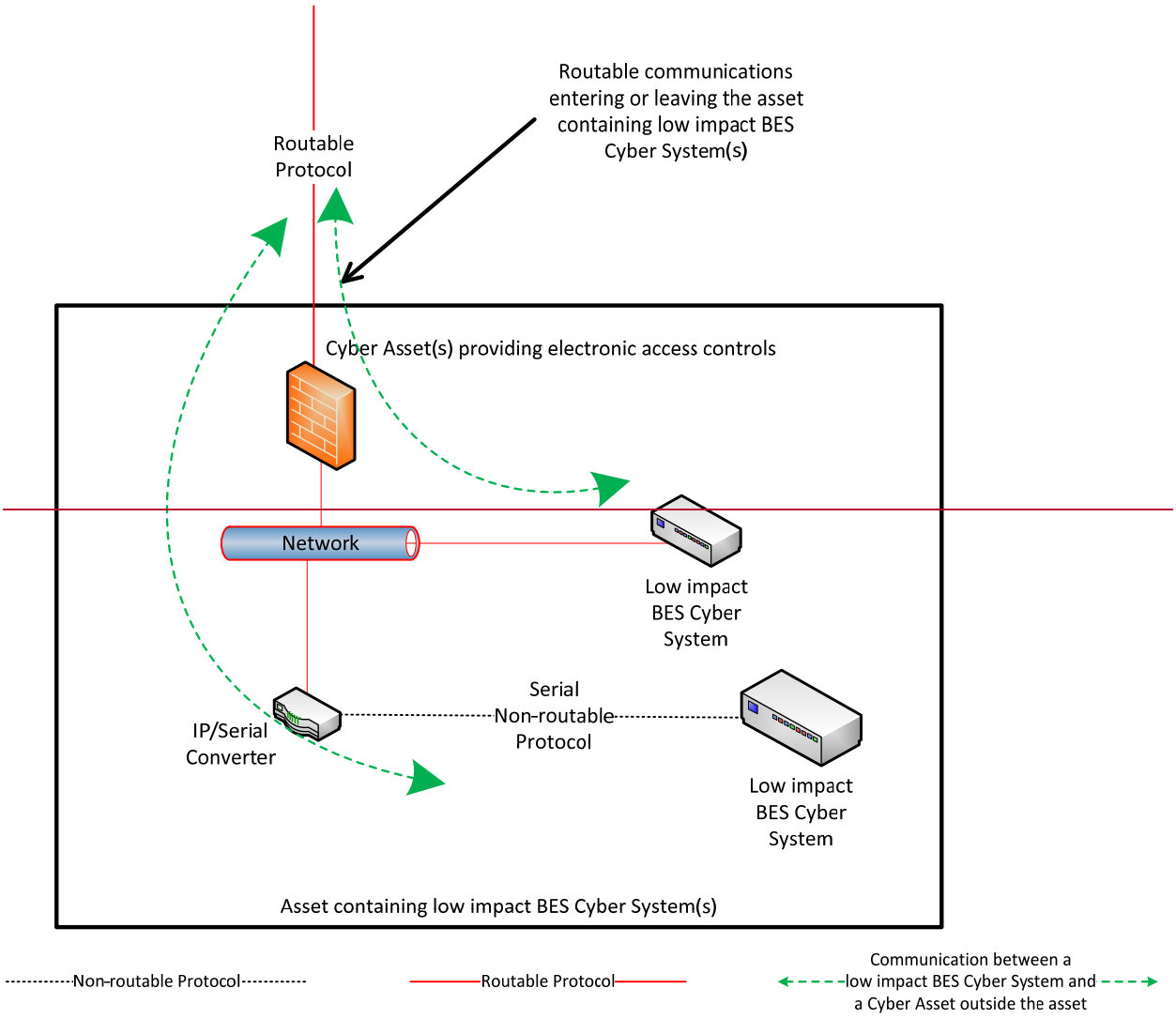
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 1~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

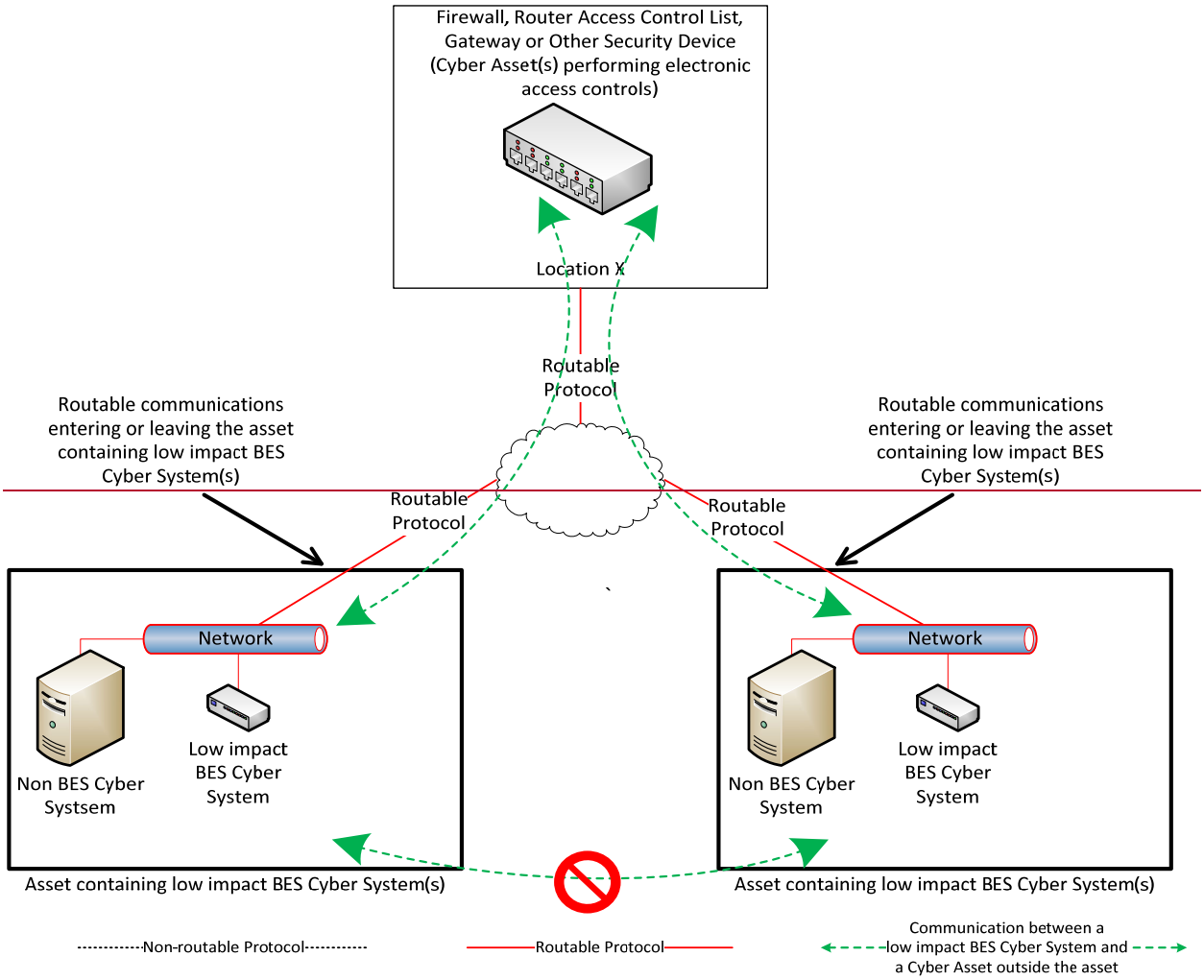
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 2~~

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

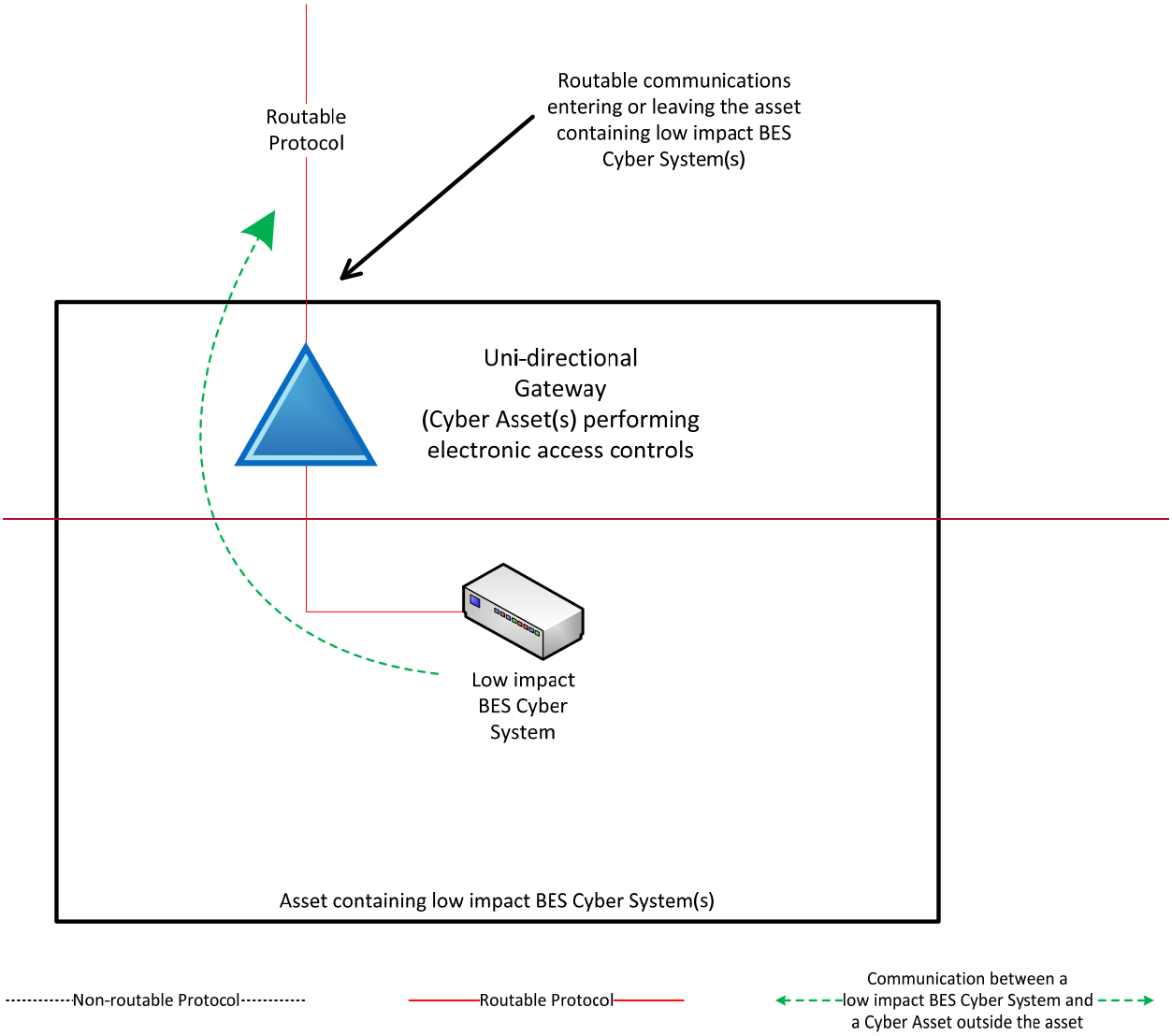
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

~~Reference Model 4 – Uni-directional Gateway~~

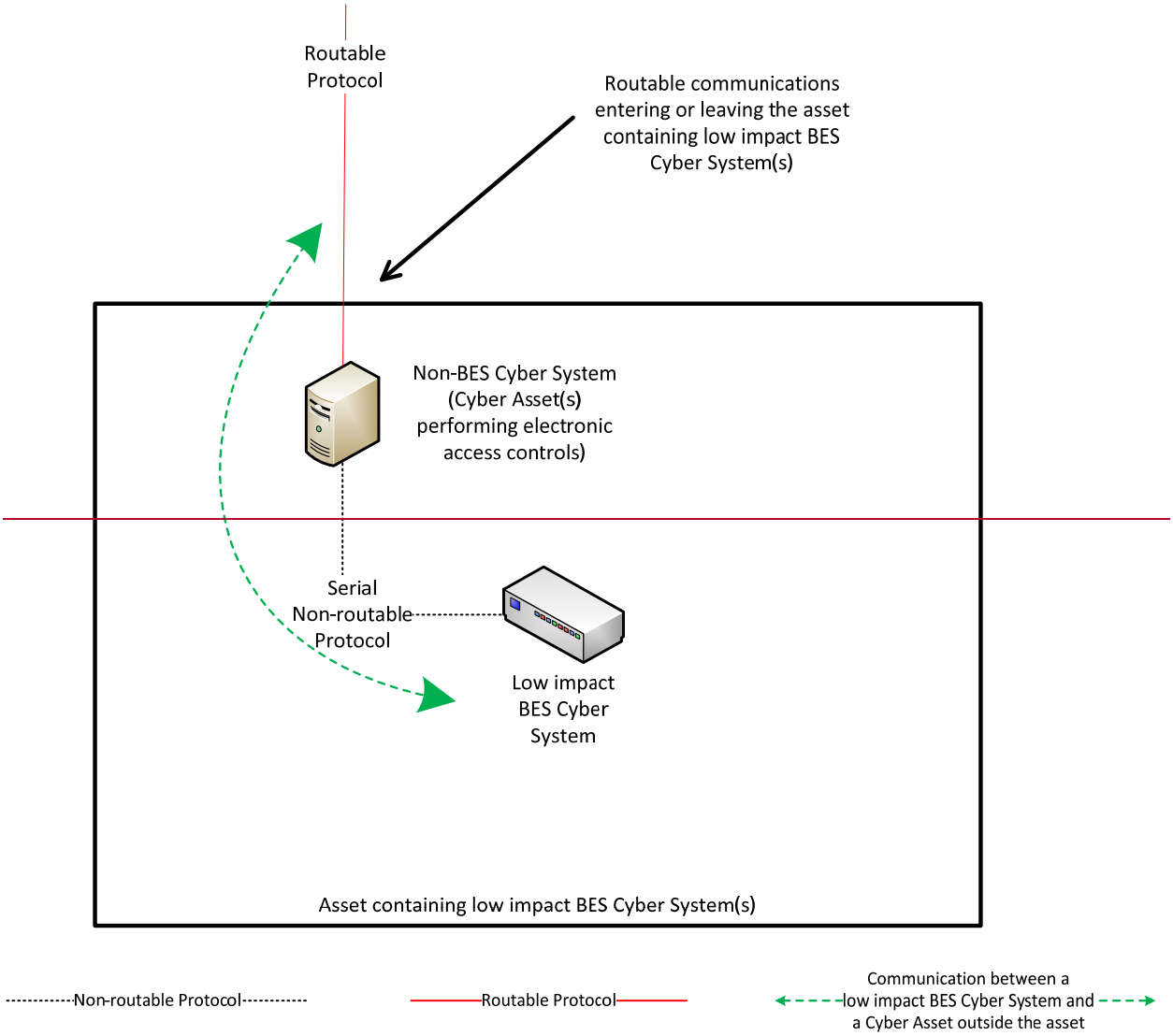
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~



~~*Reference Model 4*~~

~~Reference Model 5 – User Authentication~~

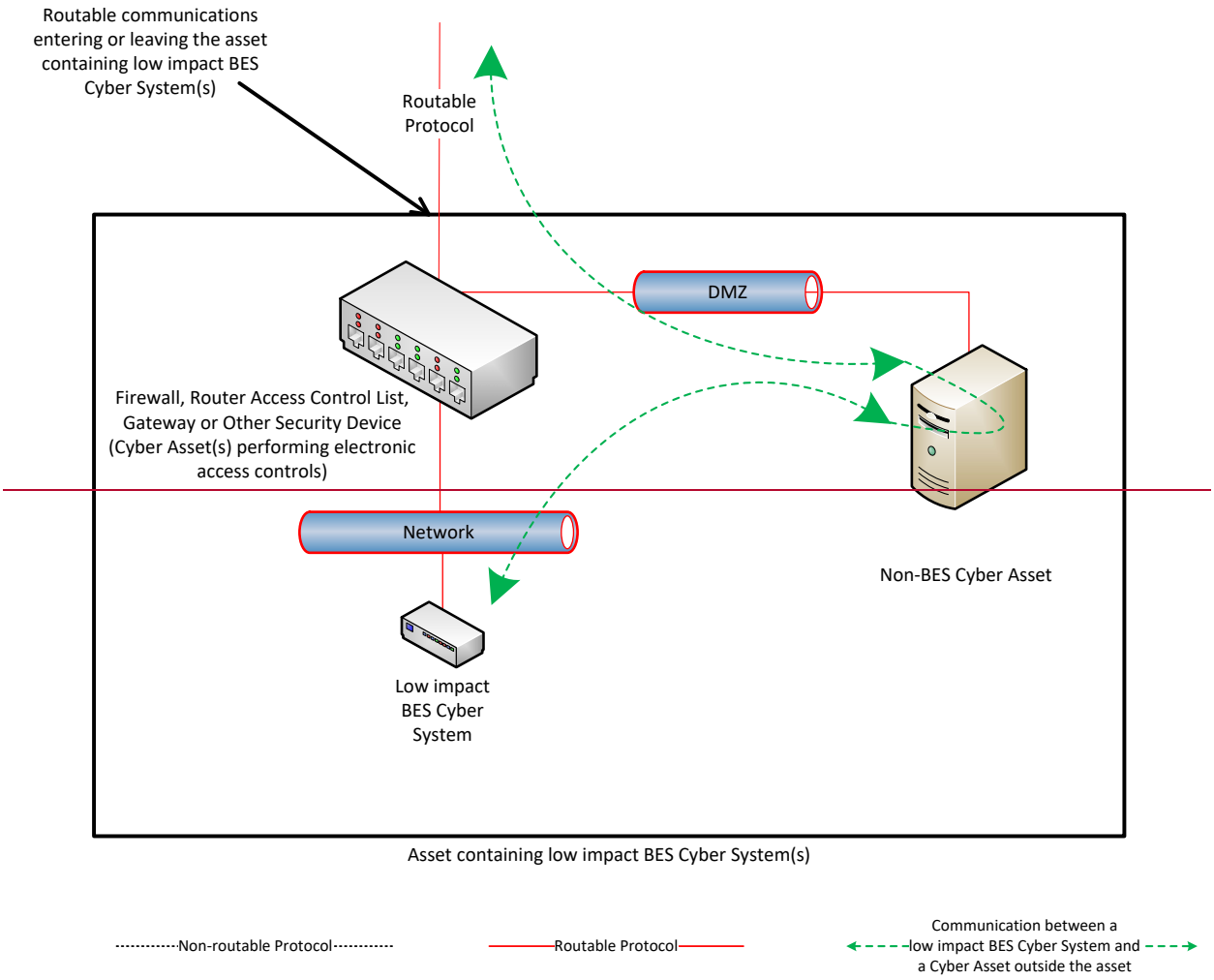
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~



~~Reference Model 5~~

~~Reference Model~~ 6 ~~— Indirect Access~~

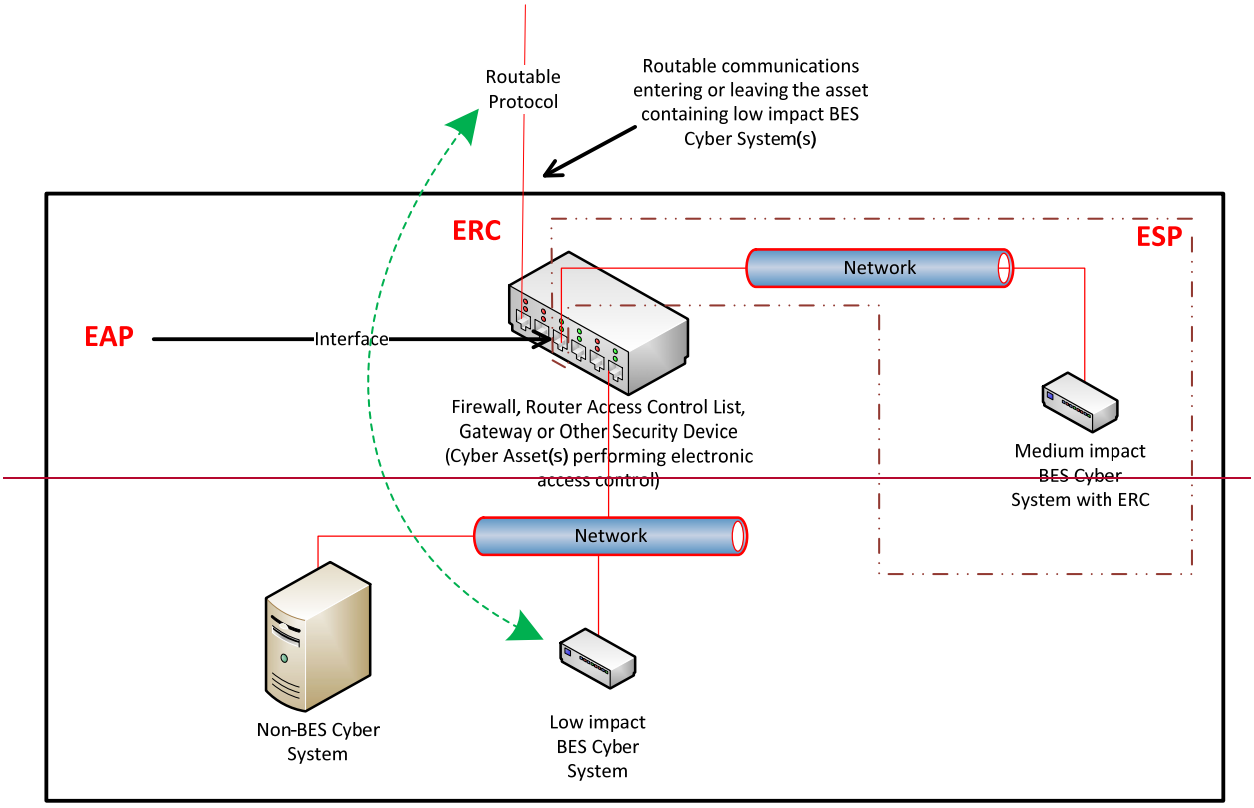
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~



~~*Reference Model 6*~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~Reference Model 7~~

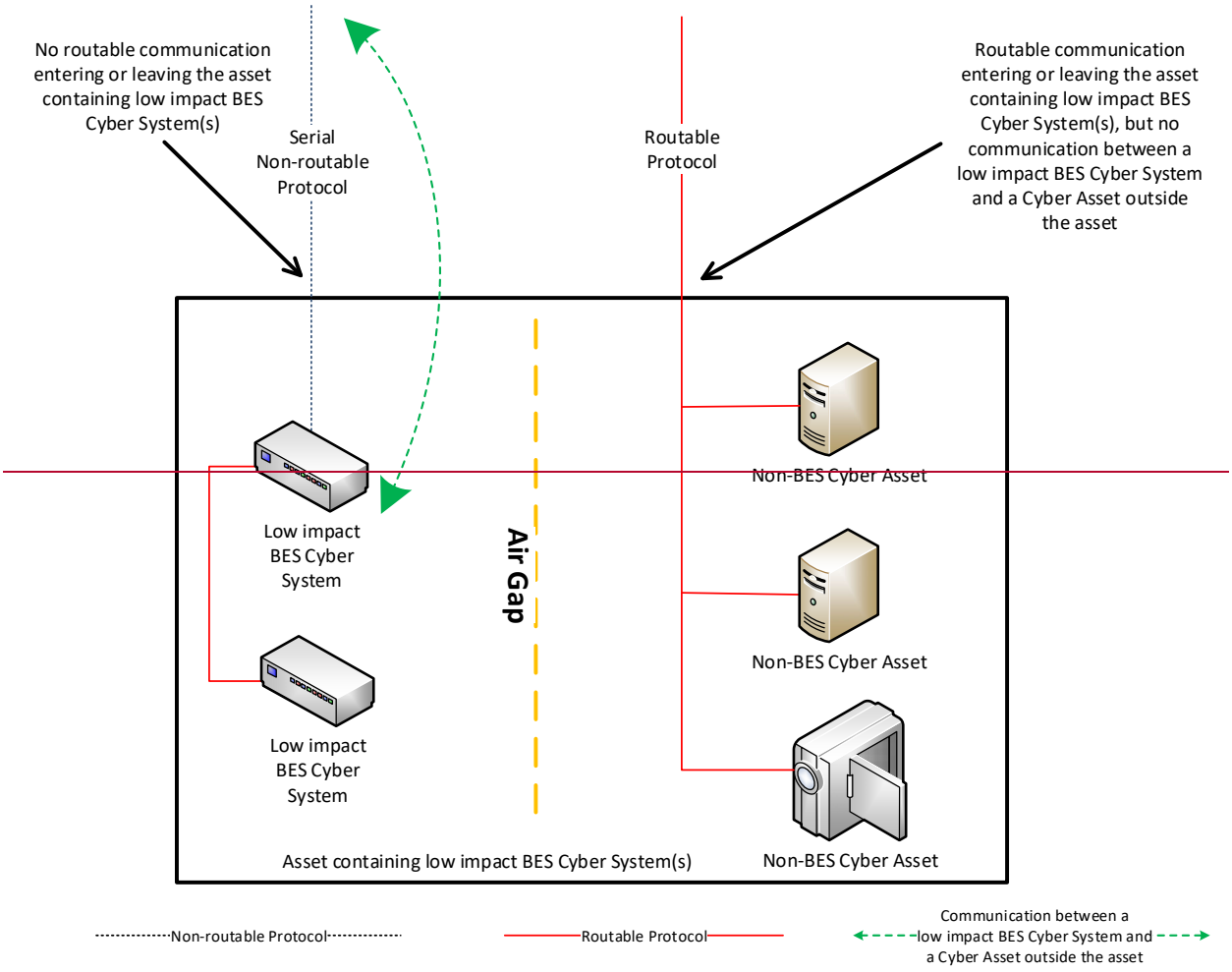
~~Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

~~1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

~~2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

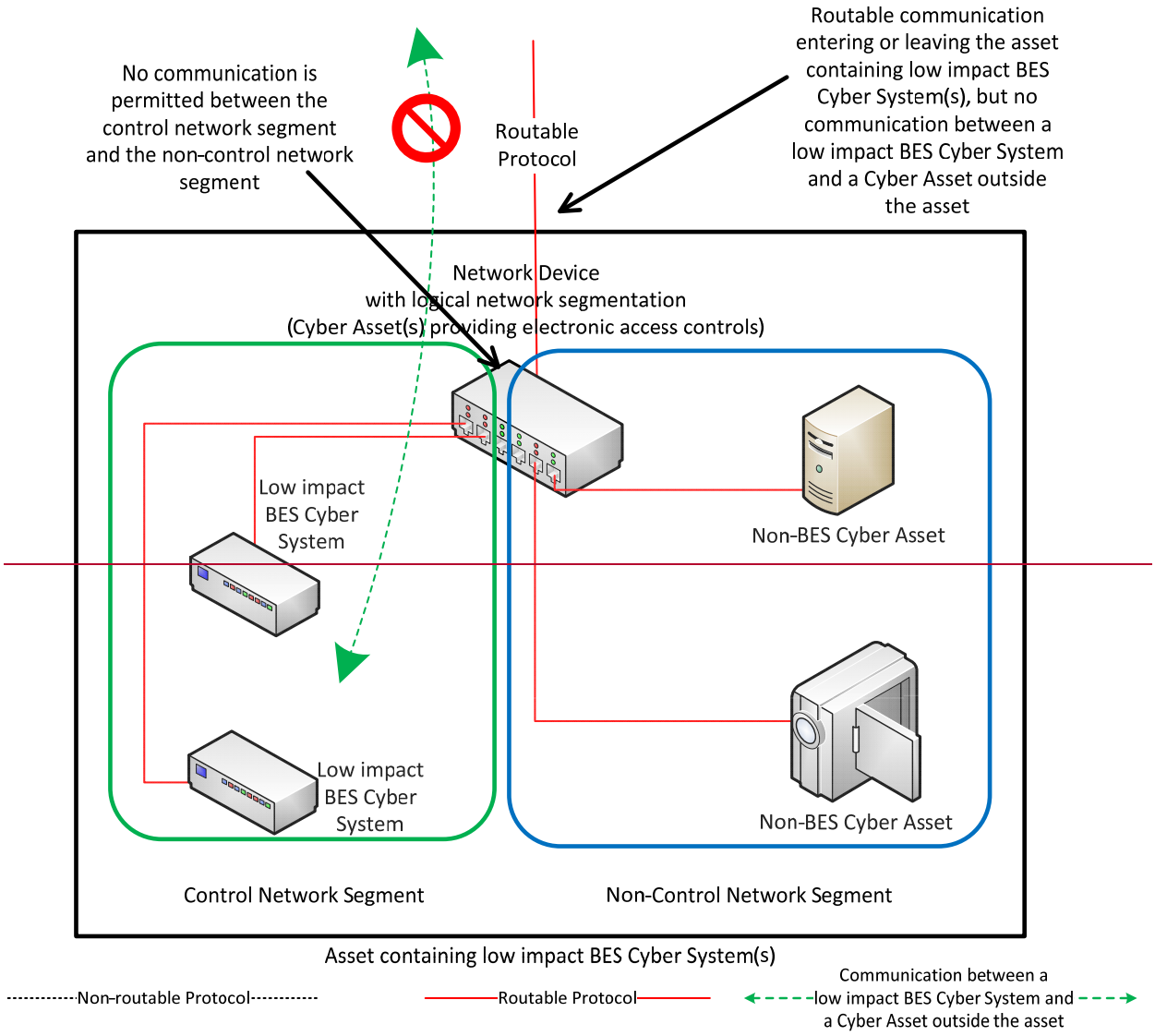
~~3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~



~~*Reference Model 8*~~

Reference Model 9 – Logical Isolation – No Electronic Access Controls Required

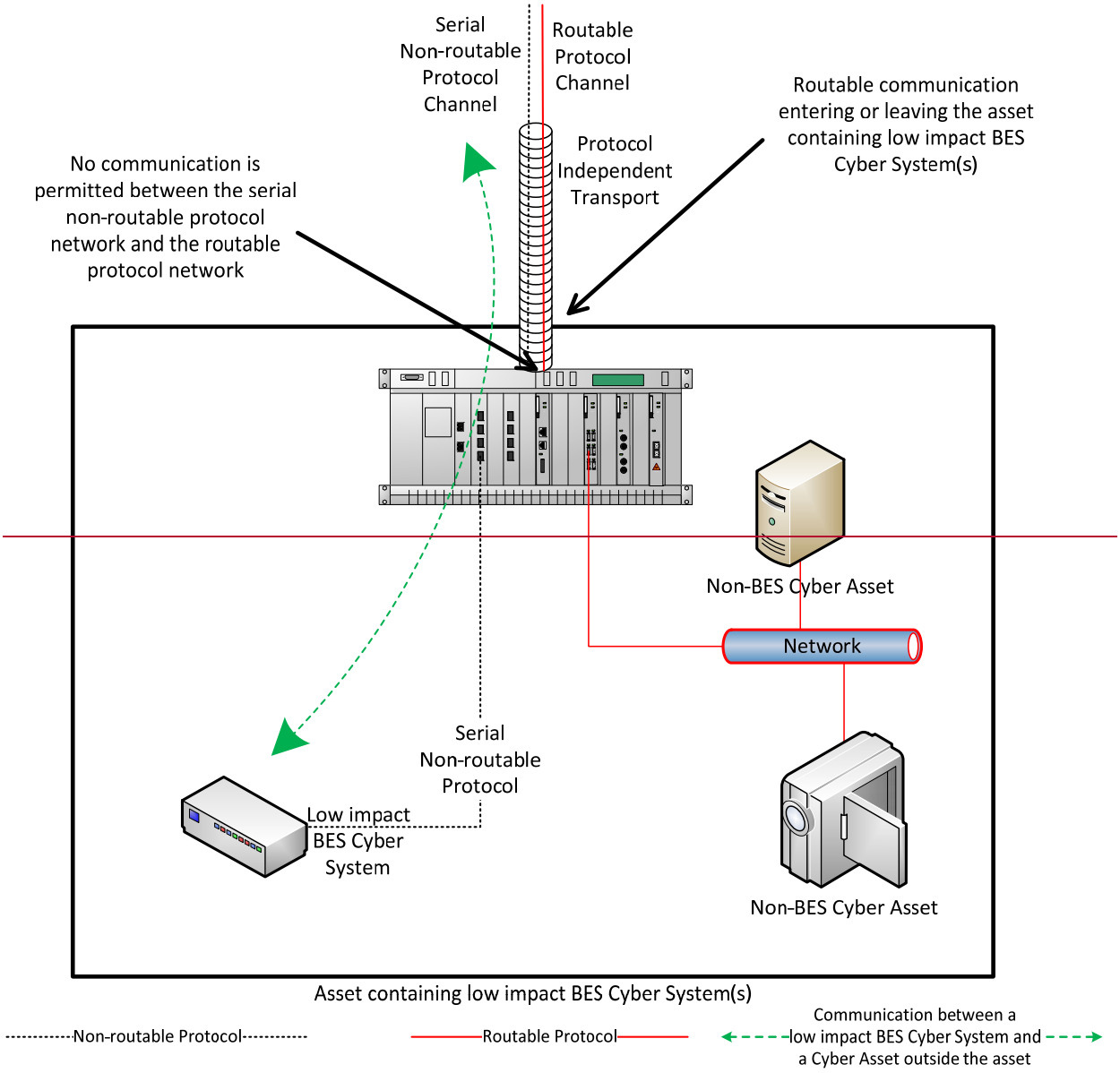
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



~~*Reference Model 9*~~

~~Reference Model 10 – Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~*Reference Model 10*~~

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to

~~disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

- ~~Diagnostic test equipment;~~
- ~~Equipment used for BES Cyber System maintenance; or~~
- ~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

Malicious Code Risk Mitigation

The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

~~The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

- ~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~
- ~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~
- ~~When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify~~

[1] ~~http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

~~the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back-up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~Section 5.2.1:~~ ~~Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

- ~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~
- ~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~
- ~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~
- ~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~
- ~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~Section 5.2.2:~~ ~~The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

~~Requirement R2, Attachment 1, Section 5.3 - Removable Media~~

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~Section 5.3:~~ ~~Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System~~

network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

1. As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous .1, documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.showing:

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is

~~named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~Annual review and approval of the cyber security policies ensures that the policies are kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~Rationale for Requirement R2:~~

~~In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

~~Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition~~

~~and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~Rationale for Section 5 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

- ~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~steps to preauthorize access;
- alerts generated by vendor log on;
- session monitoring;
- security information management logging alerts;
- time-of-need session initiation;
- session recording;
- system logs; or
- other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing:

- disabling vendor electronic remote access user or system accounts;
- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-9 — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below.

Reliability Standard CIP-003-9

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-9 shall become effective on the first day of the first calendar quarter that is 36 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

[1] See Applicability section of CIP-003-9 for additional information on Distribution Providers subject to the standard.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-9 shall become effective on the first day of the first calendar quarter that is 36 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-9 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-9.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-9 within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-9 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2020-03 Supply Chain Low Impact Revisions

Applicable Standard(s)

- CIP-003-9~~X~~ — Cyber Security — Security Management Controls

Requested Retirement(s)

- CIP-003-8 — Cyber Security — Security Management Controls

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

Effective Date and Phased-In Compliance Dates

The effective date for the proposed Reliability Standard is provided below. ~~Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The phased-in compliance date for that particular section represents the date that Responsible Entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.~~

Reliability Standard CIP-003-9~~X~~

[1] See Applicability section of CIP-003-9~~X~~ for additional information on Distribution Providers subject to the standard.

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-9~~X~~ shall become effective on the first day of the first calendar quarter that is 36 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-9~~X~~ shall become effective on the first day of the first calendar quarter that is 36 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-9~~X~~ as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.6 on or before the effective date of CIP-003-9~~X~~.

Responsible Entities shall initially comply with all other periodic requirements in CIP-003-9~~X~~ within the periodic timeframes of their last performance under CIP-003-8.

Retirement Date

Reliability Standard CIP-003-8

Reliability Standard CIP-003-8 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-9~~X~~ in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-9

October 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

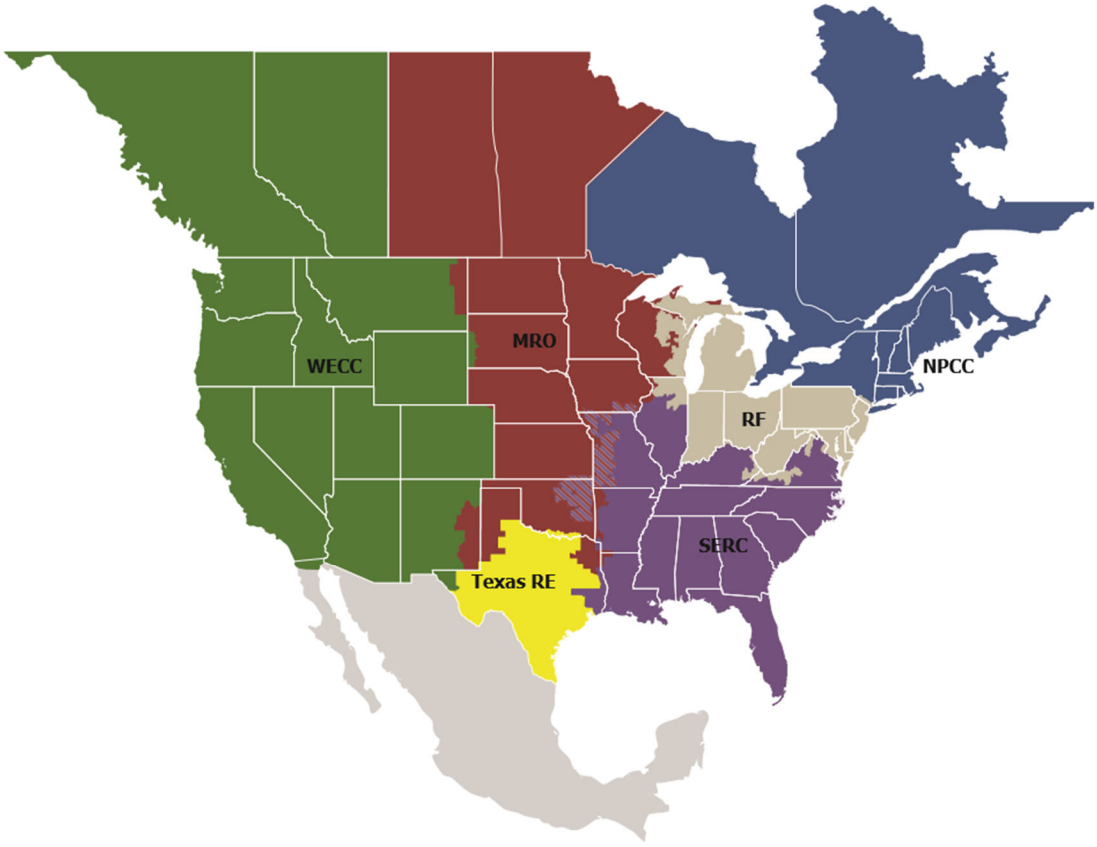
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-9

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

[1] Supply Chain Risk Assessment Report (nerc.com)
[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and

[3] CIP-013 Technical Rationale

maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-9X

~~July~~ October 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

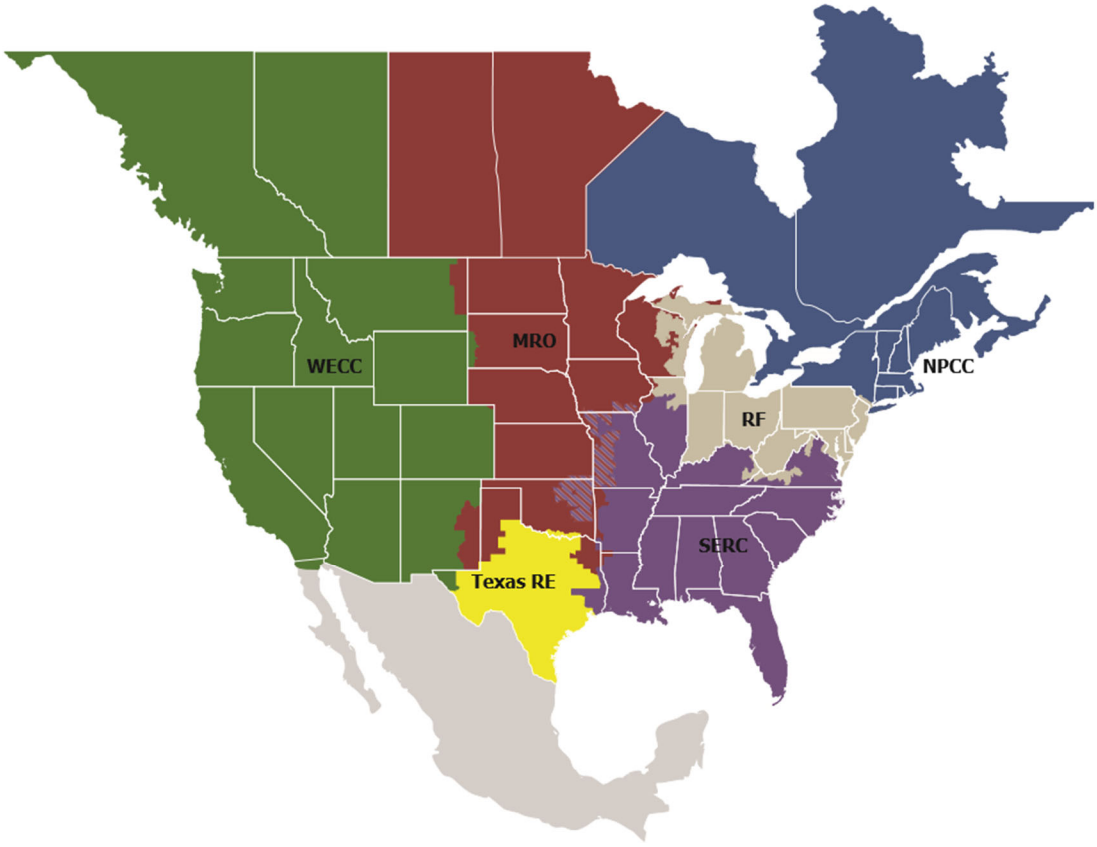
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Technical Rational for Reliability Standard CIP-003-9X

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9X is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9~~X~~ Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

[3] CIP-013 Technical Rationale

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9~~X~~ Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2020-03 Supply Chain Low Impact Revisions

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-003-9. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement
VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations
Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-003-9, Requirement R1
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1.1) OR

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR	did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR	did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR

VSLs for CIP-003-9, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was modified by adding a seventh topic to Requirement R1.2 for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to review one or more documented cyber security policies covering the topics specified in Requirement R1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-9, Requirement R2

The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low	every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement	according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity implemented vendor electronic	authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the	The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to	Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to	

VSLs for CIP-003-9, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
	document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement was not modified but the attachment referenced in the requirement was. The attachment was modified by adding a sixth section for topics that should be included in documented cyber security policies for assets identified on CIP-002 containing low impact BES Cyber Systems. The proposed VSL was modified to reflect seven topics instead of six that should be included. It does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented cyber security plans covering the sections specified in Attachment 1. Guideline 2a is not applicable as these VSLs are not binary. The VSLs do not contain ambiguous language.

VSL Justifications for CIP-003-9 Requirements R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justification for CIP-003-9, Requirement R3
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-9, Requirement R3
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VRF Justification for CIP-003-9, Requirement R4
The VRF did not change from the previously FERC approved CIP-003-8 Reliability Standard.

VSL Justification for CIP-003-9, Requirement R4
The VSL did not change from the previously FERC approved CIP-003-8 Reliability Standard.

Attachment 1

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-003-9 – Cyber Security — Security Management Controls

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Attachment 1

R4	X	*	X	X		X			X	X		

* CIP-003-9 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-003-9 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

Attachment 1

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Attachment 1

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Attachment 1

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** For its high impact and medium impact BES Cyber Systems, if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BES Cyber Systems (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets and Removable Media malicious code risk mitigation; and
  - **1.2.6.** Vendor electronic remote access security controls; and
  - **1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Attachment 1

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Attachment 1

Compliance Assessment Approach Specific to CIP-003-9, R1

This section to be completed by the Compliance Enforcement Authority

	For its high impact and medium impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Personnel and training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BES Cyber Systems (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BES Cyber Systems (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
	For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls; 4. Cyber Security Incident response 5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and 6. Vendor electronic remote access security controls; and 7. Declaring and responding to CIP Exceptional Circumstances.
	Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months.
	Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months.
	Verify the Responsible Entity has achieved the security objective of instituting cyber security policies that will preserve the availability, integrity, and confidentiality of systems that support the reliable operation of the BES.
Note to Auditor: Per Attachment 1, "Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets."	

Auditor Notes:

Attachment 1

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Attachment 1

Compliance Assessment Approach Specific to CIP-003-9, R2

This section to be completed by the Compliance Enforcement Authority

	Attachment 1, Section 1 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of ensuring personnel with access to low impact BES Cyber Systems remain aware of cyber security practices.
	Attachment 1, Section 2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to control physical access, based on need as determined by the Responsible Entity, to: 1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	Attachment 1, Section 2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to control physical access.
	Attachment 1, Section 2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of controlling physical access to: 1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	Attachment 1, Section 3.1 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to control inbound and outbound electronic access, based on need as determined by the Responsible Entity, for any communications that are: 1. Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); 2. Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and 3. Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE).
	Attachment 1, Section 3.1

	For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented its plan to control electronic access.
	Attachment 1, Section 3.1 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of permitting only necessary inbound and outbound access to its low impact BES Cyber Systems.
	Attachment 1, Section 3.2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented a plan to authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.
	Attachment 1, Section 3.2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has implemented the plan to authenticate Dial-up Connectivity.
	Attachment 1, Section 3.2 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has achieved the security objective of authenticating all Dial-up Connectivity, per Cyber Asset capability, where such connectivity permits access to its low impact BES Cyber Systems.
	Attachment 1, Section 4 For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has documented one or more Cyber Security Incident response plan(s) that include: 1. Identification, classification, and response to Cyber Security Incidents; 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law; 3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4. Incident handling for Cyber Security Incidents; 5. Testing each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and 6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 For each asset containing a low impact BES Cyber System, if the Responsible Entity responded to a Cyber Security Incident, verify the Responsible Entity implemented the Cyber Security Incident response plan.
	Attachment 1, Section 4.5 Verify the Responsible Entity tested each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or

	(3) using an operational exercise of a Reportable Cyber Security Incident.
	Attachment 1, Section 4.6 Verify the Responsible Entity updated each Cyber Security Incident response plan, if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 Verify the Responsible Entity is prepared to achieve the security objective of minimizing the adverse impact to the BES of a possible Cyber Security Incident affecting low impact BES Cyber Systems.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has documented one or more plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets.
	Attachment 1, Section 5.2.2 For any method used pursuant to 5.2.1, verify the Responsible Entity has determined whether any additional mitigation actions are necessary and has implemented such actions prior to connecting the Transient Cyber Asset.
	Attachment 1, Section 5.3.1 Verify the Responsible Entity has documented one or more plans to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System.
	Attachment 1, Section 5.3.2 Verify the Responsible Entity has documented one or more plans to mitigate the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.
	Attachment 1, Section 5.3 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Removable Media.
	Attachment 1, Section 5.3 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Removable Media.
	Attachment 1, Section 6.0 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has documented a

	process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.
	Attachment 1, Section 6.0 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has implemented a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.
	Attachment 1, Section 6.0 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, verify that the Responsible Entity has mitigated the risk associated with vendor electronic remote access, where such access has been established under Section 3.1.
	Attachment 1, Section 6.1 Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for determining vendor electronic remote access.
	Attachment 1, Section 6.2 Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for disabling vendor electronic remote access.
	Attachment 1, Section 6.3 Verify that the process documented and implemented by the Responsible Entity pursuant to section 6.0, includes one or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Note to Auditor:

Attachment 1, Section 3

1. For each asset identified as containing a low impact BES Cyber System(s) per CIP-002, the list of assets should identify those assets that have routable protocol communications between low impact BES Cyber System(s) and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions.
    a. For these identified assets, obtain as evidence the devices used to control electronic access and the low impact BES Cyber Systems for which they control access.
2. For each asset identified as containing a low impact BES Cyber System(s) per CIP-002, the Responsible Entity has an obligation to determine the necessary inbound and outbound routable protocol communications between low impact BES Cyber System(s) and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions. The Responsible Entity must be able to provide a technically sound explanation as to how its electronic access permissions and controls are consistent with the security objective of permitting only necessary inbound and outbound access to low impact BES Cyber Systems.

3. The audit team should assess the effectiveness of the Responsible Entity's electronic access control plan as well as the Responsible Entity's adherence to its electronic access control plan.
4. For the inbound and outbound communications that the Responsible Entity has determined to be necessary, the Responsible Entity must identify the electronic access controls used to effectively control access to and from the low impact BES Cyber System(s).
5. The ten reference models included in the Guidelines and Technical Basis section of the Standard provide examples that Responsible Entities may reference for their electronic access controls. Reference models 9 and 10 outline approaches for segmenting network traffic such that there is no routable protocol communications to the low impact BES Cyber System(s).
    a. Model 9 uses layer-2 network segmentation (VLANs) to control access. The configuration of the devices used to accomplish this must be documented by the Responsible Entity and assessed for its effectiveness in meeting the standard's objective of controlling access to the low impact BES Cyber System(s).
    b. In Model 10, a single device receives both serial traffic destined for low impact BES Cyber System(s) and routable traffic destined for non-BES Cyber Asset(s). The device, as depicted in the model, logically isolates the serial traffic from the routable traffic. The configurations for the device must be documented by the Responsible Entity and assessed to determine whether or not the electronic access controls effectively meet the objective of controlling access to the low impact BES Cyber System(s).

<u>Attachment 1, Section 5</u>

1. The means of verifying the mitigation of the introduction of malicious code to a low impact BES Cyber System differs depending on whether a Transient Cyber Asset is managed by the Responsible Entity in an ongoing or an on-demand manner. The verification for a Transient Cyber Asset managed in an ongoing manner focuses on the process of preventing malware from being introduced to the Transient Cyber Asset. The verification for a Transient Cyber Asset managed in an on-demand manner focuses on the process used to ensure the Transient Cyber Asset may be safely used in a low impact BES Cyber System environment prior to such use. If the Transient Cyber Asset is managed in both an ongoing and an on-demand manner, then both verification techniques should be employed.

Auditor Notes:

_____

Attachment 1

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-9, R3

This section to be completed by the Compliance Enforcement Authority

	Verify the CIP Senior Manager has been identified by name.
	Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change.
	Verify the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Auditor Notes:

Attachment 1

Attachment 1

R4 Supporting Evidence and Documentation

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-9, R4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented a process to delegate authority, unless no delegations are used.
	Verify that all delegates have been identified by name or title.
	Verify that the delegation of authority includes the specific action delegated.
	Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP

	Standards.
	Verify that the dates for all delegations have been recorded.
	Verify that the CIP Senior Manager approved all delegations.
	Verify that any changes made to delegations were dated and documented within 30 days of the change.
Note to Auditor: Delegations of the CIP Senior Manager's authority are permitted for the required approvals in CIP-002-5.1, Requirement R2, CIP-007-6, Requirement R2, Part 2.4, and CIP-013-1 R3.	

Auditor Notes:

Attachment 1

Additional Information:

Reliability Standard

The full text of CIP-003-9 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 706
See FERC Order 791
See FERC Order 822
See FERC Order 843
See FERC Letter Order in Docket RD19-5-000 Dated July 31, 2019

Attachment 1

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Removable Media

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a:
    - BES Cyber Asset,
    - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
    - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
    - BES Cyber Asset,
    - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
    - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:

  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and

  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented

prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
    - other operational, procedural, or technical controls.
3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies (e.g., full packet inspection technologies);
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	9/9/2019	CCTF	New document based on CIP-003-7 RSAW

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2020-03 Supply Chain Low Impact Revisions

Final Ballot Open through November 4, 2022

Now Available

A final ballot for **CIP-003-9 - Cyber Security — Security Management Controls** is open through **8 p.m. Eastern, Friday, November 4, 2022.**

Project 2016-02 (Virtualization) and Project 2020-03 (Supply Chain) have both made modifications to CIP-003. In previous postings, the Supply Chain team is used“-X" in place of the version number, and Virtualization used “-Y". In preparation for the filing with the NERC Board of Trustees, Supply Chain has updated the version number to CIP-003-9.

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pool(s) associated with this project can log into the Standards Balloting and Commenting System (SBS) and submit votes here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process
For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2020-03 Supply Chain Low Impact Revisions CIP-003-X FN 4 ST
Voting Start Date: 10/26/2022 12:28:51 PM
Voting End Date: 11/4/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 4
Total # Votes: 251
Total Ballot Pool: 291
Quorum: 86.25
Quorum Established Date: 10/26/2022 3:53:48 PM
Weighted Segment Value: 68.95

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	78	1	50	0.758	16	0.242	0	3	9
Segment: 2	6	0.1	1	0.1	0	0	0	3	2
Segment: 3	69	1	41	0.695	18	0.305	0	4	6
Segment: 4	20	1	8	0.533	7	0.467	0	2	3
Segment: 5	64	1	36	0.692	16	0.308	0	3	9
Segment: 6	47	1	25	0.714	10	0.286	0	3	9
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	1	0	0	0	0	0	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	5	0.4	3	0.3	1	0.1	0	1	0
Totals:	291	5.5	164	3.792	68	1.708	0	19	40

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	N/A
1	City Utilities of Springfield, Missouri	Mike Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Negative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	Pjoy Chua		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Negative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Salt River Project	Sarah Blankenship		Negative	N/A
1	Santee Cooper	Chris Wagner		Negative	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	N/A
1	Taunton Municipal Lighting Plant	Devon Tremont		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	None	N/A
1	Wind Energy Transmission Texas, LLC	doug whitworth		None	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Harishkumar Subramani Vijay Kumar		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	N/A
3	Cowlitz County PUD	Russell Noble		Negative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Abstain	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Negative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Negative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Negative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Maria Pardo		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Public Utility District No. 1 of Pend Oreille County	Philip Roice		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Negative	N/A
3	Santee Cooper	James Poston		Negative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Wabash Valley Power Association	Scott Berry		Negative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	American Public Power Association	John McCaffrey		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	DTE Energy	Patricia Ireland		Negative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Krys Rootham		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Arevon Energy	Srinivas Kappagantula		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Christopher Siewert		Negative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		None	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	N/A
5	Lakeland Electric	George Kerst		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young	Helen Zhao	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	John Cook	Scott Brame	Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Negative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Negative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Negative	N/A
5	Santee Cooper	Marty Watson		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright	Megan Caulson	None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	LaKenya Vannorman	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Negative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 1 of Pend Oreille County	April Owen		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Negative	N/A
6	Santee Cooper	Glenda Horne		Negative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		None	N/A
9	British Columbia Utilities Commission	Sarosh Muncherji		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 291 of 291 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit H

Standard Drafting Team Roster, Project 2020-03
Supply Chain Low Impact Revisions

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2020-03 Supply Chain Low Impact Revisions

	Name	Entity
Chair	Tony Hall	LG&E and KU Energy
Vice Chair	Kevin Conway	Pend Oreille County Public Utility District No. 1
Members	Jeffery Sweet	AEP
	Harold Sherrill	RWE Renewables Americas
	Barry Jones	WAPA
	John C. Grube	Duke Energy – Midwest Regional Services
	Roy Kiser	Southern Company
	Joseph Gatten	Xcel Energy
	Karl Perman	CIP Corps
	Shannon Ferdinand	Capital Power
	Ida Mauricio	CPS Energy
	Steven Briggs	Tennessee Valley Authority
PMOS Liaison	Masuncha Bussey	Duke Energy
NERC Staff	Alison Oswald – Senior Standards Developer	North American Electric Reliability Corporation
	Laura Anderson – Standards Developer (Support)	North American Electric Reliability Corporation
	Marisa Hecht – Legal	North American Electric Reliability Corporation