

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability
Standard CIP-013-3

January 2021

RELIABILITY | RESILIENCE | SECURITY



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

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3.....	3
Introduction.....	3
New and Modified Terms and Applicability	3
Requirement R1.....	3
Technical Rationale for Reliability Standard CIP-013-2.....	4
Introduction.....	4
New and Modified Terms Used on NERC Reliability Standards	4
Requirement R1 and R2.....	4
Requirement R3.....	7
Technical Rationale for Reliability Standard CIP-013-1.....	8
Rationale.....	8

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. 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-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team’s (SDT’s) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry’s implementation activities. During the course of the V5TAG’s activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, “The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.”

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-013-3 for virtualization, the SDT added SCI as applicable in Requirement R1. Note that Management Modules of SCI are not added as these are included components that are already covered under of the procurement of the SCI.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a “cut and paste” of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

- (1) Software integrity and authenticity;
- (2) Vendor remote access;
- (3) Information system planning; and
- (4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report ¹(Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

¹ NERC, “Cyber Security Supply Chain Risks, Staff Report and Recommended Actions”, May 17, 2019.

[https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20\(20190517\).pdf](https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf)

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "...the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "...to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"².

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "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." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various

² NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019.

[https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20\(20190517\).pdf](https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf)

functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

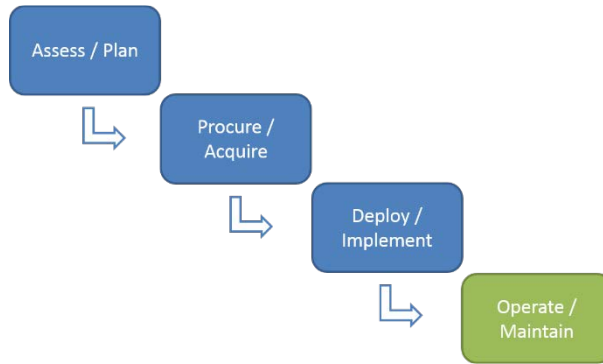
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

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.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

- (1) Software integrity and authenticity;
- (2) Vendor remote access;
- (3) Information system planning; and
- (4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

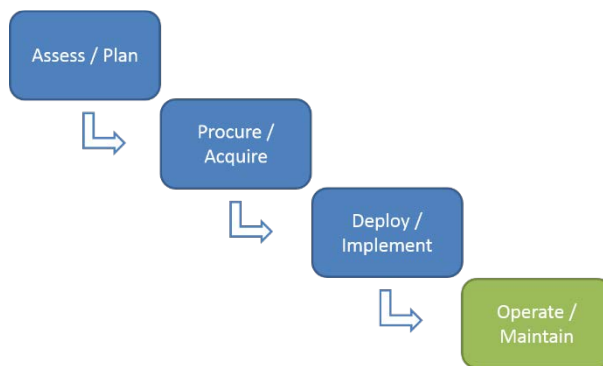
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires

entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

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.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).