UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Michael Mabee	**)**	**Docket No. EL20-46-000**
Complainant	**)**	
	)	
v.	**)**	
	)	
Federal Energy Regulatory Commission	**)**	

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Shamai Elstein
Assistant General Counsel
Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
shamai.elstein@nerc.net
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

June 11, 2020

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Michael Mabee	)	**Docket No. EL20-46-000**
Complainant	)	
	)	
v.	)	
	)	
Federal Energy Regulatory Commission	)	

MOTION TO INTERVENE AND COMMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 206, 212, and 214 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Rules of Practice and Procedure[1] and the Commission's Notice of Complaint,[2] the North American Electric Reliability Corporation ("NERC") moves to intervene and comment on the Complaint filed by Michael Mabee ("Complainant") on May 12, 2020 in the above-captioned docket ("Complaint").

The Complaint claims that (i) Critical Infrastructure Protection ("CIP") Reliability Standard CIP-013-1 – Cyber Security Supply Chain Risk Management does not comport with Presidential Executive Order 13920: Securing the United States Bulk-Power System (the "BPS Executive Order");[3] and (ii) that the CIP Reliability Standards do not fully address the National Institute of Standards and Technology ("NIST") Cybersecurity Framework.[4] The Complaint

[1] 18 C.F.R. §§ 385.206, 385.212, and 385.214 (2019).
[2] Notice of Complaint, Docket No. EL20-46-000 (May 14, 2020).
[3] Executive Order 13920 of May 1, 2020, *Securing the United States Bulk-Power System*, 85 Fed. Reg. 26595 (May 4, 2020).
[4] *NIST*, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

requests the Commission (i) issue a public notice of the Complaint; (ii) investigate the Complaint; and (iii) direct NERC to make modifications to CIP-013-1 and other CIP Reliability Standards.

As discussed below, NERC requests leave to intervene and comment in response to the Complainant's assertions and recommendations, and requests that the Commission dismiss the Complaint.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[5]

Shamai Elstein*
Assistant General Counsel
Lauren Perotti*
Senior Counsel
Marisa Hecht*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
shamai.elstein@nerc.net
lauren.perotti@nerc.net
marisa.hecht@nerc.net

II. MOTION TO INTERVENE

NERC has a substantial interest in this proceeding as the Complainant seeks to have the Commission direct NERC to modify the CIP-013-1 Reliability Standard and other CIP Reliability Standards.[6] By enacting the Energy Policy Act of 2005,[7] Congress entrusted the Commission with

[5] 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.

[6] Complaint at 6-7.

[7] 16 U.S.C. § 824o (2018).

the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System ("BPS"), and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. The Commission certified NERC as the ERO in 2006.[8]

As the ERO, NERC's mission is to improve the reliability and security of the BPS in North America.[9] Under its FERC-approved Rules of Procedure, NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure ("ROP") and the NERC Standard Processes Manual ("SPM").[10] NERC and the Regional Entities are responsible for monitoring, assessing, and enforcing compliance with Reliability Standards in the United States in accordance with Section 400 (Compliance Enforcement) of the ROP and the NERC Compliance Monitoring and Enforcement Program.[11]

No other party can adequately represent NERC's interests or adequately respond to Complainant's allegations regarding CIP-013-1 and other CIP Reliability Standards. Therefore, it is in the public interest to permit this intervention.

---

[8] *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on compliance*, 118 FERC ¶ 61,190, *order on reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[9] *See id.*

[10] The NERC Rules of Procedure are available at https://www.nerc.com/AboutNERC/Pages/Rules-ofProcedure.aspx. The NERC Standard Processes Manual is available at https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

[11] *Id.* The NERC Compliance Monitoring and Enforcement Program is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf.

III. SUMMARY

A. Summary of the Complaint

The Complainant alleges that the CIP-013-1 Reliability Standard does not comport with the BPS Executive Order and that FERC has not ensured that mandatory CIP Reliability Standards fully address leading federal cyber security guidance, specifically the NIST framework.[12] The Complainant recommends that the Commission:

i. Issue public notice of the complaint;

ii. Investigate the complaint;

iii. Direct NERC to modify CIP-013-1 to cover all equipment in the BPS, including low impact BES Cyber Systems; and

iv. Direct NERC to revise CIP standards to "fully address" federal guidance for cybersecurity, specifically NIST.[13]

B. Summary of NERC's Comments

The Commission should dismiss the Complaint because it fails to meet the minimum requirements applicable to complaints under the Commission's Rules of Practice and Procedure.[14] Rule 203, for example, requires pleadings to set forth the basis in fact and law for the positions taken.[15] Rule 206 provides eleven elements that a complaint must contain, including the following, among others: (a) clearly identify the alleged action or inaction claimed to violate applicable statutory or regulatory requirements, (b) set forth the business, commercial, economic, or other issues presented by the action or inaction "as such relate to or affect the complainant," (c) indicate

---

[12] NERC notes that the Complainant, as a private citizen, is not subject to the NERC Reliability Standards, including the CIP Reliability Standards.

[13] Complaint at 6-7.

[14] *See* 18 C.F.R. § 385.206.

[15] 18 C.F.R. § 385.203(a)(7).

the practical, operational, or other nonfinancial impacts imposed as a result of the action or inaction, including, where applicable, the environmental, safety or reliability impacts of the action or inaction; and (d) make a good faith effort to quantify the financial impact or burden created for the complainant due to the action or inaction.[16] Long-standing Commission precedent provides that "rather than bald allegations, [a complainant] must make an adequate proffer of evidence including pertinent information and analysis to support its claims."[17]

The Complainant has failed to demonstrate that Reliability Standard CIP-013-1 does not comport with the BPS Executive Order or is otherwise inconsistent with applicable statutory and regulatory law. As discussed further below, the BPS Executive Order complements CIP-013-1 and affirms NERC's approach to help manage supply chain risks. As the BPS Executive Order works in concert with CIP-013-1, the Complainant offers no other new information to justify the Commission reconsidering its determination that CIP-013-1 is just, reasonable, not unduly discriminatory or preferential, and in the public interest.

Additionally, NERC currently is revising the CIP Reliability Standards to address certain of the supply chain risks raised by the Complainant. Consistent with FERC and the NERC Board of Trustees direction, NERC is in the process of developing modifications to the CIP Reliability Standards to expand the scope of NERC's supply chain standards to address supply chain risks for

[16] 18 C.F.R. § 385.206(b) (listing the full list of elements for a complaint) (NERC does not waive objection to the Complaint's failure to meet other elements of a properly pleaded complaint but is simply highlighting these elements).

[17] *Ill. Muni. Elec. Agency v. Cent. Ill. Pub. Serv. Co.*, Order Dismissing Complaint Without Prejudice, 76 FERC ¶ 61,084 at 4 (1996); *CAlifornians for Renewable Energy, Inc., (CARE) and Barbara Durkin v. Nat'l Grid, Cape Wind, and the Mass. Dep't of Pub. Util.*, Order Dismissing Complaint, 137 FERC ¶ 61,113, at PP 2, 31-32 (2011); *CAlifornians for Renewable Energy, Inc., Michael E. Boyd, and Robert M. Sarvey v. Pac. Gas and Elec. Co.*, Order Dismissing Complaint, 143 FERC ¶ 61,005 at P2 (2013); and *Citizens Energy Task Force and Save Our Unique Lands v. Midwest Reliability Org., et al.*, Order Dismissing Complaint, 144 FERC ¶ 61,006, at P 38 (2013).

low impact BES Cyber Systems and to broaden the applicable systems for medium and high impact BES Cyber Systems.

NERC also takes a defense-in-depth approach by engaging in activities in addition to mandatory Reliability Standards to help industry mitigate supply chain risks. These efforts include alerts to industry on emerging supply chain risks, an initiative dedicated to supply chain risk mitigation, discussions at grid security exercises, and collaboration with industry stakeholders. These efforts complement the BPS Executive Order.

Furthermore, the Complaint's unsupported assertions regarding use of the NIST framework reflect the Complainant's misunderstanding of the NERC standards development process and other activities supporting the reliability of the BPS. Contrary to the Complainant's assertions, NERC used the NIST framework to inform development of the currently effective CIP standards and continues to use the framework to inform further updates and improvement. Likewise, the Commission often references the NIST framework in its issuances regarding the CIP Reliability Standards and other Commission activities. NERC recognizes the importance of the NIST Cybersecurity Framework and works to ensure all elements of the NIST framework's voluntary efforts are taken into consideration and tracked to all mandatory CIP standards.

In sum, the Complaint fails to (i) substantiate its claims; (ii) clearly state any impacts or issues that relate to the Complainant caused by NERC's activities; and (iii) provide remedies that are not already underway. For these reasons, the Commission should decline to provide the relief requested by the Complainant.

IV. COMMENTS

A. The Complainant has failed to demonstrate that Reliability Standard CIP-013-1 does not comport with the BPS Executive Order or is otherwise inconsistent with applicable statutory and regulatory law.

The Complaint asserts that the BPS Executive Order invalidates the approach in CIP-013-1 and requests that the Commission direct further modifications to the standard.[18] The Complainant has failed to meet its burden under the Commission's rules. The Complainant does not provide proof or specific examples as to how the BPS Executive Order invalidates the approach used in CIP-013-1. Instead, the Complainant relies on a logical fallacy that because the BPS Executive Order covers more systems than CIP-013-1, the BPS Executive Order does not comport with and invalidates the approach used in CIP-013-1.[19] To the contrary, CIP-013-1 is complementary to the BPS Executive Order, as described below. Because the Complainant has failed to support its assertions, as required by the Commission's rules and regulations, the Complaint should be dismissed.

The following brief comparison of the BPS Executive Order and the CIP Reliability Standards demonstrates that the CIP Reliability Standards and the BPS Executive Order are complementary.

The BPS Executive Order "prohibits Federal agencies and U.S. persons from acquiring, transferring, or installing BPS equipment in which any foreign country or foreign national has any interest and the transaction poses an unacceptable risk to national security or the security and safety of American citizens."[20] Furthermore, the BPS Executive Order authorizes the Secretary of Energy

---

[18] Complaint at 3-4.

[19] *Id*.

[20] *Department of Energy*, Press Release, President Trump Signs Executive Order Securing the United States Bulk-Power System (May 1, 2020), https://www.energy.gov/articles/president-trump-signs-executive-order-securing-united-states-bulk-power-system.

to take actions to implement the order and states the Secretary of Energy, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other agencies, "shall publish rules or regulations implementing the authorities delegated to the Secretary by this order" within 150 days of the date of the BPS Executive Order.[21]

Reliability Standard CIP-013-1 requires Responsible Entities[22] to develop and implement plans to address supply chain cybersecurity risks during the planning and procurement of high and medium impact BES Cyber Systems. As stated in the petition for approval, the security objective of the supply chain cybersecurity risk management plans is to ensure that Responsible Entities consider the security, integrity, quality, and resilience of the supply chain and take appropriate mitigating action when procuring BES Cyber Systems to address threats and vulnerabilities in the supply chain.[23] The supply chain cybersecurity risk management plans must include processes to: (1) identify and assess cybersecurity risks to the BES from vendor products and services; and (2) include specified security concepts in their procurement activities for high and medium impact BES Cyber Systems, including (i) vendor security event notification processes, (ii) coordinated incident response activities, (iii) vendor personnel termination notification for employees with access to remote and onsite systems, (iv) vulnerability disclosures, (v) software integrity and authenticity, and (vi) coordination of controls for vendor remote access.[24]

---

[21] BPS Executive Order, 85 Fed. Reg. at 26596.

[22] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

[23] *Petition of NERC for Approval of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Docket No. RM17-13-000, p. 13 (Sep. 26, 2017) ("NERC Petition").

[24] *Id*. at pp. 13-14.

Additionally, supply chain requirements in CIP-005-6 and CIP-010-3 address specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.[25] Pursuant to Requirement R2, Parts 2.4 and 2.5 of Reliability Standard CIP-005-6, Responsible Entities must have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5).[26] The security objective of these requirement parts is to control vendor remote access to mitigate risks associated with unauthorized access.[27]

As described above, the CIP Reliability Standards speak to supply chain risks generally, whereas the BPS Executive Order addresses specific risks from specific sources (e.g., hostile governments). Rather than invalidating the risk-based approach in CIP-013-1, the BPS Executive Order works in concert with NERC's supply chain standards to help mitigate supply chain management risks in the electric industry. For instance, NERC expects Responsible Entities to assess the risks detailed in the BPS Executive Order when planning for procurement of high and medium impact BES Cyber Systems as part of their CIP-013-1 processes. Similarly, any future regulations or guidelines developed pursuant to the BPS Executive Order will need to be factored into the processes required under CIP-013-1. In this way, the efforts outlined in the BPS Executive Order will help support the actions required by CIP-013-1. Security of the BPS requires a multi-pronged approach, and pursuit of one action, such as the items outlined in the BPS Executive Order, does not mean that other actions, such as the risk assessment process under CIP-013-1, are invalidated or unnecessary. In fact, as described above, they work together to help mitigate supply chain risks to the BPS.

---

25 *Id.*
26 *Id.*
27 *Id.*

Further, the Complainant has not demonstrated a deficiency in the applicable statutory and regulatory processes used for the development and approval of CIP-013-1. NERC developed Reliability Standard CIP-013-1 in accordance with its open and inclusive, Commission-approved standard development process.[28] On July 21, 2016, the Commission issued an order 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 operations.[29] Reliability Standard CIP-013-1, along with revisions to CIP-005-5 and CIP-010-2, was developed in response to the Commission's directive. As explained in detail in NERC's petition for approval of the standards,[30] Reliability Standard CIP-013-1 addressed the Commission's directive in Order No. 829. Following a public rulemaking process, the Commission found that Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 satisfied its directives in Order No. 829 and approved the standard as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[31]

For these reasons, the Commission should dismiss the Complaint. The Complaint is deficient because it does not offer any evidence that the BPS Executive Order is an "indictment of lack of action on part of FERC and the ERO"[32] and does not demonstrate how the standard or the

---

[28] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual, available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

[29] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050, at P 43 (2016) ("Order No. 829").

[30] *Petition of NERC for Approval of Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, Docket No. RM17-13-000 (Sep. 26, 2017) ("NERC Petition").

[31] *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 at P 28 (2018) ("Order No. 850"). Rather than repeat the justifications for the applicability and each of the individual requirements of the CIP-013-1, CIP-005-6, and CIP-010-3 standards here, NERC refers the Commission to the record of Docket No. RM17-13-000.

[32] Complaint at 3.

actions of FERC and NERC are inconsistent with applicable law, as is the required burden for a complaint. Aside from these unsupported assertions, the Complainant offers "no new information to justify revisiting [the] determination"[33] that CIP-013-1 is just, reasonable, not unduly discriminatory or preferential, and in the public interest "or to exercise [the Commission's] authority under section 215(d)(5) of the [Federal Power Act] to direct modifications"[34] to CIP-013-1.

B. NERC is addressing the issues raised in the Complaint regarding CIP-013-1, so the relief sought by Complainant is already underway.

The Complaint requests that the Commission direct NERC to modify CIP-013-1 to cover "every piece of equipment in the [BPS]."[35] NERC continues to evaluate the Supply Chain Standards to ensure that appropriate systems are covered, based on risk to the BPS.

For example, Project 2019-03 – Cyber Security Supply Chain Risks is proposing to include additional applicable systems to address Commission directives[36] and NERC staff recommendations[37] based on careful analysis of the potential risks and vulnerabilities of specific systems. The additional applicable systems include Electronic Access Control or Monitoring Systems and Physical Access Control Systems for medium and high impact BES Cyber Systems. In addition, further work is underway in Project 2020-03 – Supply Chain Low Impact Revisions

---

33 *Complaint of Michael Mabee Related to Critial Infrastructure Reliability Standard*, Order Denying Complaint, 171 FERC ¶ 61, 205 at P 11 (2020).

34 *Id*.

35 Complaint at 6.

36 Order No. 850 at P 46.

37 NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 2019), https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Supply%20Chain%20Report%20Filing.pdf; filed in Docket No. RM17-13-000.

to expand CIP-003 to provide specific protections to low impact systems to address the areas of greatest risk posed by such systems.[38]

Several of the Complainant's recommendations for changes to CIP-013-1 resemble those already being considered by current standards development projects, as described above. The Commission should allow NERC to consider these changes through its Commission-approved open and inclusive development process, subject to the necessary technical analysis and stakeholder scrutiny, before directing any further changes in response to an unsubstantiated Complaint. NERC's risk-based approach is preferable to the Complainant's request that FERC direct NERC to revise CIP-013-1 to cover "every piece of equipment in the BPS" as it helps ensure that resources are allocated to address systems that present higher level risks to BPS reliability.

C. NERC supports activities beyond mandatory Reliability Standards to help mitigate supply chain risks.

NERC notes that Reliability Standards are just one tool NERC uses to support mitigation of supply chain risks and to help to ensure the reliability and security of the BPS. As shown by the following excerpt from the 2019 State of Reliability Report, a combination of activities supporting a defense-in-depth approach to supply chain risk mitigation has helped avoid cyber or physical security incidents on BES facilities that resulted in a loss of load:

> In 2018, as in previous years, there were no reported cyber or physical security incidents on BES facilities that resulted in a loss of load. This is the single most important security measure because it shows that the combined efforts of industry, NERC, the E-ISAC,

[38] Information on Project 2020-03 is available on the project page, https://www.nerc.com/pa/Stand/Pages/Project_2020-03_Supply_Chain_Low_Impact_Revisions.aspx.

> and government partners have so far been successful in protecting the BPS's reliability.[39]

While mandatory Reliability Standards play an integral role in securing the BPS, NERC recognizes the importance of multiple approaches in supporting supply chain risk mitigation, such as the BPS Executive Order. At NERC's May 2020 Board of Trustees meeting,[40] Bruce Walker, assistant secretary for the Office of Electricity at the Department of Energy ("DOE"), stated that the BPS Executive Order builds upon the significant ongoing work of NERC, FERC, and industry.[41] Speaking to implementation, Mr. Walker noted that DOE will continue the collaborative work with FERC, NERC, and the Electricity Subsector Coordinating Council in a targeted, thoughtful manner.[42]

In addition to its mandatory Reliability Standards, the following NERC activities, initiatives, and actions help address supply chain risk management and support the goal of continuing to avoid cyber or physical security incidents on BES facilities that result in loss of load:

- Supply Chain Risk Mitigation Program: In addition to supporting the implementation of the supply chain standards, the Supply Chain Risk Mitigation Program,[43] adopted as resolutions by the NERC Board, includes the following efforts to enhance reliability through mitigation of supply chain risks:
  1. Performed cyber security supply chain risk study and engaged EPRI to perform an independent assessment of supply chain risks;
  2. Communicates supply chain risks to industry;
  3. Requested forums and trade associations to develop white papers addressing best and leading practices for supply chain management; and
  4. Evaluates the effectiveness of supply chain standards.

---

[39] NERC State of Reliability Report at 67, https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf.

[40] *NERC*, Press Release, Response to White House Executive Order (May 1, 2020), https://www.nerc.com/news/Pages/Response_to_White_House_Executive_Order.aspx.

[41] *NERC*, Announcement, Board Holds Virtual Meeting; Approves Updated Align Timeline, SEL Strategy (May 14, 2020) at 2, https://www.nerc.com/news/Headlines%20DL/Board%2014MAY20.pdf.

[42] *Id*.

[43] The website for the Supply Chain Risk Mitigation Program is available at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

- Data Requests, Assessments, and Reports:
  - NERC analyzes supply chain risk through assessments and other reports, such as the Special Report: Pandemic Preparedness and Operational Assessment: Spring 2020 and State of Reliability Reports.[44]
  - To better understand supply chain risks, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure.[45] NERC analyzed the data received to understand the implications of supply chain vulnerabilities not covered in CIP-013-1, CIP-005-6, and CIP-010-3, producing a final report.[46]
- NERC Alerts:[47] NERC has issued two supply chain alerts within the past few years, with another Alert being developed:
  - In October 2017, NERC issued a non-public Level 2 NERC Alert regarding supply chain risk, specifically stakeholders' use of Kaspersky anti-virus software.
  - In March 2020, NERC issued a public Level 2 NERC Alert that provided a recommendation regarding supply chain disruptions as a result of coronavirus disease.[48]
  - NERC is preparing a Level 2 NERC Alert requiring registered entities to report on equipment used that is banned by the BPS Executive Order.
- GridEx: E-ISAC included a supply chain topic in NERC's Grid Security Exercise, GridEx IV.
- NERC Reliability and Security Technical Committee ("RSTC"): In 2019, the RSTC Supply Chain Working Group developed several guidelines regarding supply chain security and a widely distributed "letter to industry" with information for industry

---

[44] NERC, *Special Report, Pandemic Preparedness and Operational Assessment* (Spring 2020), Special Report: Pandemic Preparedness and Operational Assessment: Spring 2020; State of Reliability Reports are available at https://www.nerc.com/pa/RAPA/PA/Pages/default.aspx.

[45] NERC, *Request for Data or Information: Supply Chain Risk Assessment Data Request* (August 2019): https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Final%201600%20data%20request%20-%20clean.pdf.

[46] NERC, *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (December 2019), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf. NERC recommended revising CIP-013-1 in this report, although ultimately the Board resolved to revise CIP-003-8.

[47] The Complainant cited an exchange between NERC Chief Executive Officer Jim Robb and Senator Angus King during a public hearing of the Senate Committee on Energy and Natural Resources regarding NERC's knowledge of the brands of equipment used on the BPS. (Complaint at 2). Mr. Robb began explaining the importance of a NERC Alert on this topic but was redirected prior to finishing his response to Senator King. As a result, the cited exchange did not capture the value of NERC Alerts in both disseminating and collecting information regarding supply chain issues.

[48] NERC, *Recommendation to Industry: Coronavirus Disease (COVID-19) Pandemic Contingency Planning* (Mar. 10, 2020) https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC_Alert_R-2020-03-10-01_COVID-19_Pandemic_Contingency_Planning.pdf.

suppliers. In 2020, more guidelines are expected as well as a webinar series that features discussions about each guideline.

These activities demonstrate that NERC employs a comprehensive approach to accomplish its mission of maintaining a reliable BPS in the face of supply chain threats.

D. The Complainant has failed to demonstrate NERC or FERC did not "fully address" the NIST framework in developing the CIP Reliability Standards.

The Complainant also fails to substantiate its claim that "The Federal Energy Regulatory Commission (FERC) has not ensured that mandatory CIP standards 'fully address leading federal guidance for critical infrastructure cybersecurity—specifically, the National Institute of Standards and Technology (NIST) Cybersecurity Framework' "[49] in an appropriate manner.[50] Complainant cites to House Subcommittee statements from 2008 that refer to previous versions of the CIP Reliability Standards and a United States Government Accountability Office ("GAO") Report on Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid ("GAO Report").[51]

NERC consistently relies upon the NIST framework to inform its cybersecurity standards development efforts. As NERC noted in its response to the GAO Report, NERC recognizes the importance of the NIST Cybersecurity Framework and works to ensure all elements of the NIST framework's voluntary efforts are taken into consideration and tracked to all mandatory CIP Reliability Standards.[52] In the past, NERC staff has worked with its stakeholder technical committees to develop a high-level comparison of the CIP Reliability Standards to the NIST

---

[49] Complaint at 1, 4.
[50] Complaint at 4.
[51] *GAO*, Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid (August 2019), https://www.gao.gov/assets/710/701079.pdf.
[52] *Id*. at p. 74 (Appendix V).

framework in a guideline that has since been retired.[53] This retired guideline demonstrated a large degree of overlap between the NIST framework and the CIP Reliability Standards. Currently, NERC staff is working with a RSTC working group to develop an updated mapping of the CIP Reliability Standards to the NIST framework.

It is important to recognize that NERC standards and the NIST framework serve different purposes (mandatory versus voluntary for Responsible Entities), and NERC tailors any concepts from the NIST framework for this purpose. As such, there will not be a complete overlap from the voluntary framework to the mandatory requirements. Nonetheless, as evidenced by the record for several CIP standards, NERC relies heavily on the NIST framework to develop its mandatory Reliability Standards, and the CIP "Version 5" standards drew concepts from the NIST framework.[54] Moreover, current CIP standards development projects use NIST to inform the development of the requirements.[55] NERC will continue to draw from NIST in its future development projects.

Similarly, the Commission often references the NIST framework in its issuances regarding the CIP Reliability Standards. For example, in Order No. 706 directing revisions to version 1 of the CIP Reliability Standards, the Commission stated, "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP

---

53 CIPC Control Systems Security Working Group, Mapping of NIST Cybersecurity Framework to NERC CIP v3/v5 (retired) (November 2014), https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/CSSWG-Mapping_of_NIST_Cybersecurity_Framework_to_NERC_CIP.pdf.

54 *See* Docket No. RM13-5-000.

55 DRAFT Technical Rationale for CIP-011-3, https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_Technical%20Rationale_CIP-011-3_201912.pdf (references NIST practices for media sanitization and data retrieval).

Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework."[56] In addition to referencing the NIST framework in its issuances, the Commission invited a NIST staff member to provide input on supply chain risk management during a technical conference regarding the CIP Reliability Standards.[57] These two examples, among others, demonstrate the Commission considers the concepts within the NIST framework when addressing the CIP Reliability Standards. As such, the Complainant's assertion that the Commission has not ensured that the NIST framework is "fully addressed" is unfounded when the Commission has consistently focused on the NIST framework as a valuable resource for CIP Reliability Standards development.

Moreover, the Commission considered how version 5 of the CIP Reliability Standards addressed NIST guidance, seeking comment on "whether, and in what way, adoption of certain aspects of the NIST Risk Management Framework could improve the security controls proposed in the CIP version 5 Standards."[58] In subsequent Order No. 791, the Commission directed some revisions to the CIP Reliability Standards based on NIST while declining to direct certain other modifications, instead directing FERC staff to convene a technical conference to discuss the NIST framework.[59] Based on these actions, the Commission demonstrates it continuously addresses the NIST framework and its relationship to the CIP Reliability Standards.

---

[56] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 at P 25 (2008) ("Order No. 706"), *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[57] *In the matter of Supply Chain Risk Management*, Transcript of the 1/28/16 technical conference held in Washington, DC re Supply Chain Risk Management under RM15-14, Docket No. RM15-14-000 pp. 23-28 (2016).

[58] *Version 5 Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 143 FERC ¶ 61,055 at P 117 (2013).

[59] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), order on clarification and reh'g, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

Finally, NERC observes that the assertions in the Complaint regarding the NIST framework could have been raised in comments submitted during NERC's open and inclusive standard development process,[60] or the Commission's own public rulemaking processes, where they could have been addressed on the record. The failure to do so then does not provide the grounds for a complaint now.

V. CONCLUSION

WHEREFORE, for the reasons stated above, NERC respectfully requests that the Commission grant this motion to intervene, accept the comments herein, and dismiss the Complaint.

[60] Indeed, NERC notes that its process allows any stakeholder to submit a new request to revise a standard through its standard development process. No such request has been submitted by the Complainant for Reliability Standard CIP-013-1.

Respectfully submitted,

/s/ Marisa Hecht

Shamai Elstein
Assistant General Counsel
Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
shamai.elstein@nerc.net
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: June 11, 2020

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a copy of this document upon all parties listed on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Washington, D.C., this 11th day of June, 2020.

/s/ Marisa Hecht
Marisa Hecht
Counsel for the North American Electric Reliability Corporation