173 FERC ¶ 61,010
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Richard Glick and James P. Danly.

Complaint of Michael Mabee
Related to Critical Infrastructure
Reliability Standards

Docket No. EL20-46-000

ORDER DENYING COMPLAINT

(Issued October 2, 2020)

1. On May 12, 2020, Michael Mabee filed a complaint (Complaint) under section 215 of the Federal Power Act (FPA)[1] and Rule 206 of the Commission's Rules of Practice and Procedure.[2] The Complaint alleges that Reliability Standard CIP-013-1 (Cyber Security Supply Chain Risk Management) does not comport with Presidential Executive Order 13,920 and that the Critical Infrastructure Protection (CIP) Reliability Standards do not fully address the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[3] The Complaint requests that the Commission direct the North American Electric Reliability Corporation (NERC) to correct these deficiencies. For the reasons discussed below, we deny the Complaint.

## I. Background

### A. Supply Chain Risk Management Reliability Standards

2. NERC submitted the supply chain risk management Reliability Standards for approval in response to a Commission directive in Order No. 829.[4] On October 18, 2018, in Order No. 850, the Commission approved the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber

[1] 16 U.S.C. § 824o.

[2] 18 C.F.R. § 385.206 (2020).

[3] Complaint at 1.

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

Security – Configuration Change Management and Vulnerability Assessments).[5] In addition to approving Reliability Standard CIP-013-1, Order No. 850 directed NERC to develop and file modifications to include Electronic Access Control and Monitoring Systems associated with medium and high impact BES Cyber Systems[6] within the scope of the supply chain risk management Reliability Standards.[7] The Commission also accepted NERC's commitment to evaluate the supply chain risks presented by Physical Access Control Systems and Protected Cyber Assets.[8]

3. Reliability Standard CIP-013-1 requires responsible entities to develop one or more documented supply chain cybersecurity risk management plans for high and medium impact BES Cyber Systems. Responsible entities must identify whether their BES Cyber Systems are "high" or "medium" impact using the identification and categorization process required by CIP-002-5.1a (Cyber Security — BES Cyber System Categorization). BES Cyber Systems are categorized as "low" impact by default if they do not meet the criteria of Reliability Standard CIP-002-5-1a.

### B. Presidential Executive Order 13,920: Securing the United States Bulk-Power System

4. On May 1, 2020, the President issued an Executive Order on securing the United States Bulk-Power System. The order highlights the risk of foreign adversaries creating and exploiting vulnerabilities in the Bulk-Power System and includes several prohibitions related to Bulk-Power System equipment. Among other things, the Executive Order restricts any acquisition, importation, transfer, or installation of Bulk-Power System equipment if that equipment was "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign

---

[5] *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020, at P 5 (2018).

[6] NERC defines bulk electric system (BES) Cyber System as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." In turn, NERC defines BES Cyber Asset as "[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. …" NERC Glossary of Terms Used in Reliability Standards.

[7] Order No. 850, 165 FERC ¶ 61,020 at P 5.

[8] *Id.* P 6.

adversaries…"[9] The Executive Order directs the Department of Energy to develop regulations to protect the Bulk-Power System from supply chain-related threats.[10]

### C. NIST Framework

5. NIST is a part of the U.S. Department of Commerce that advances measurement science, standards, and technology. On April 16, 2018, NIST published Version 1.1 of its voluntary Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework).[11] The document provides industry standards, guidelines, and practices to allow organizations to manage cybersecurity risks to critical infrastructure.

## II. Complaint

6. The Complaint contends that Reliability Standard CIP-013-1 does not comport with Executive Order 13,920 because the Reliability Standard excludes low impact BES Cyber Systems. The Complaint alleges that the Executive Order is a "vote of no-confidence" in the actions of the Commission and NERC to address cyber threats. The Complaint states that NERC has "demonstrated a lack of urgency" addressing supply chain issues.[12] And the Complaint asserts that Reliability Standard CIP-013-1 fails to cover all BES Cyber Systems despite "the protest of numerous commenters" as the Reliability Standard applies to only high and medium impact systems.[13] Further, the Complaint avers that identifying a BES Cyber Asset as low impact is left to the discretion of the responsible entity.[14] The Complaint requests the Commission direct NERC to modify Reliability Standard CIP-013-1 to include all Bulk-Power System equipment without exclusions.

7. The Complaint also contends that the Commission has not ensured the CIP Reliability Standards fully address the NIST Framework. The Complaint supports its assertion by citing to a variety of resources, including a congressman's House

---

[9] Exec. Order No. 13,920, 85 Fed. Reg. 26,595 (May 4, 2020).

[10] *See* Dept. of Energy, Request for Information, 85 Fed. Reg. 41,023 (July 8, 2020) (the public comment period ended Aug. 24, 2020).

[11] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[12] Complaint at 2.

[13] *Id.* at 3.

[14] *Id.*

subcommittee statements from 2008[15] and a 2019 Government Accountability Office (GAO) report noting the extent to which the NERC Reliability Standards address the NIST Framework's identify and protect functions.[16] The Complaint warns that there have already been threats to the supply chain from state actors and requests the Commission direct NERC to modify the CIP Reliability Standards to fully address the NIST Cybersecurity Framework.[17]

8. Complainant also submitted a motion on May 13, 2020 (May 13 Motion) to prevent the Edison Electric Institute from intervening in this proceeding and to require intervenors to certify they lack "affiliation, members, interests or shareholders who are entities or governments that are a foreign adversary as defined in Executive Order 13920."[18]

## III. Notice of Filing and Responsive Pleadings

9. Notice of the Complaint was published in the *Federal Register*, 85 Fed. Reg. 30,691 (May 20, 2020), with interventions and protests due on or before June 11, 2020. A timely motion to intervene was filed by Public Citizen, and timely motions to intervene and comment were filed by NERC, Secure the Grid Coalition, John Appelbaum, George Cotter, and jointly by the American Public Power Association (APPA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), Large Public Power Council (LPPC), and National Rural Electric Cooperative

[15] Complaint at 4 (citing *Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid: Hearing Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology*, Serial No. 110-117, 110th Cong. (2008) (statement from Rep. James R. Langevin)).

[16] *Id.* (citing GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332, at 47 (Aug. 26, 2019)).

[17] *Id.* at 6.

[18] May 13 Motion at 5. Complainant filed a second motion on June 5, 2020, requesting that the Commission take notice of two supply chain-related press reports. We have considered those materials in this proceeding.

Association (NRECA), (collectively, Trade Associations). On June 25, 2020, George Cotter filed a second out-of-time comment.[19]

## IV. Comments

10. NERC, the Trade Associations, and Appelbaum filed comments in opposition to the assertions made in, and the relief sought by, the Complaint. NERC and the Trade Associations contend that the Complainant failed to demonstrate that Reliability Standard CIP-013-1 does not comport with the Executive Order or is otherwise inconsistent with applicable statutory and regulatory law.[20] The Trade Associations add that the Complaint's claim that there is discretion in deciding what is a low impact BES Cyber System is inaccurate.[21] NERC also notes that it is already undertaking activities to address issues raised in the Complaint and discusses multiple activities it engages in beyond those in the Reliability Standards to mitigate risks to the supply chain.[22] NERC states that it continues to ensure it considers and tracks the NIST Framework to all mandatory CIP Reliability Standards.[23] Both the Trade Associations and Appelbaum maintain that until there is action by the Secretary of Energy to define foreign adversaries or specific equipment needing scrutiny, there is no support for the Complaint's assertion that Reliability Standard CIP-013-1 is inconsistent with the Executive Order.[24]

11. Secure the Grid Coalition and Cotter support the assertions contained in, and the relief sought by, the Complaint. Additionally, Secure the Grid Coalition requests that the Commission require any electric power research organization (e.g., the Electric Power Research Institute) seeking to intervene in this proceeding to "certify that it has no affiliation, members, interests or shareholders who are entities or governments that are a foreign adversary as defined in Executive Order 13920."[25]

---

[19] While Cotter's first comments addressed supply chain issues raised in the Complaint, the second comments filed June 25, 2020, are largely directed at other docketed proceedings before the Commission.

[20] NERC Comments at 7; Trade Associations Comments at 7.

[21] Trade Associations Comments at 7.

[22] NERC Comments at 11-14.

[23] *Id.* at 16-17.

[24] Trades Associations Comments at 5; Appelbaum Comments at 3-4.

[25] Secure the Grid Comments at 1.

## V. Determination

### A. Procedural Matters

12. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2020), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

13. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214, the Trade Associations' motion to intervene is granted given their interest in this proceeding as representatives of registered entities that are subject to the Commission-approved Reliability Standards.

14. Rule 213(a)(2) of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.213(a)(2) (2020), prohibits an answer to a protest or answer unless otherwise ordered by the decisional authority. We are not persuaded to accept Cotter's June 25 submission and will, therefore, reject it. As mentioned above, these comments do not address the substance of the immediate proceeding.

### B. Substantive Matters

15. As discussed below, we deny the Complaint because the relief sought therein is either unsupported or premature given current proceedings before the Commission and projects within NERC.

16. The Complaint does not provide any legal basis to conclude that Executive Order 13,920 "invalidates" or otherwise requires modifications to Reliability Standard CIP-013-1 "to cover every piece of equipment in the bulk power system with no exceptions."[26] Nothing in the Executive Order purports to direct such action by the Commission.

17. Moreover, the Commission has recently issued a Notice of Inquiry seeking comments on the potential risks to the BES posed by using equipment and services

[26] While Reliability Standard CIP-013-1 does not apply to low impact BES Cyber Systems, the Complaint incorrectly asserts that "the discretion is left to the individual companies in the industry to decide what is 'low impact.'" *Id.* at 3. In fact, Reliability Standard CIP-002-5.1 a (Cyber Security – BES Cyber System Categorization) establishes bright-line thresholds for BES Cyber Systems that must be designated as high or medium impact. Only those BES Cyber Systems that do not qualify as high or medium are categorized as low impact.

produced or provided by entities identified as risks to national security.[27] The Notice of Inquiry seeks comments on whether the current CIP Reliability Standards adequately mitigate the identified risks and comments on possible actions to consider taking to address the identified risks.

18. The relief sought in the Complaint is also premature given the ongoing efforts by NERC to address supply chain risks for low impact BES Cyber Systems. As NERC explains in its comments, it is currently revising the CIP Reliability Standards to expand protections for low impact BES Cyber Systems and broaden the applicable systems for medium and high impact BES Cyber Systems.[28]

19. We similarly deny the Complaint's request to direct NERC to revise the CIP Reliability Standards to "fully address" federal guidance for cybersecurity (i.e., NIST Framework). NERC explains in its comments that it looks to the NIST Framework to inform NERC's efforts in the development of CIP Reliability Standards,[29] and we have similarly emphasized the importance of considering voluntary standards by NIST since first approving the CIP Reliability Standards.[30]

20. The Commission has also initiated a proceeding to address potential gaps between the NIST Framework and the CIP Reliability Standards. On June 18, 2020, the Commission issued a Notice of Inquiry seeking comments on potential gaps between the NIST Framework and the CIP Reliability Standards.[31] As noted in the Notice of Inquiry, Commission staff undertook a review of the NIST Framework and identified topics that

---

[27] *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, 172 FERC ¶ 61,224 (2020).

[28] NERC Comments at 5-6.

[29] NERC Comments at 15 (explaining NERC "consistently relies upon the NIST framework to inform its cybersecurity standards development efforts").

[30] *See e.g., Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at P 233, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No, 706-B, 126 FERC ¶ 61,229, *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009) (directing NERC to monitor the development and implementation of cyber security standards by NIST to "determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards…").

[31] *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, 171 FERC ¶ 61,215 (2020).

may not be adequately addressed in the CIP Reliability Standards.[32] The Notice of Inquiry comments will assist the Commission in assessing the need for potential enhancements to the currently-effective CIP Reliability Standards in view of the NIST Framework.

The Commission orders:

We deny the Complaint, as discussed in the body of this order.

By the Commission.

( S E A L )

Kimberly D. Bose,
Secretary.

[32] The Notice of Inquiry observed that the Commission, going back to the approval of the first version of the CIP Reliability Standards in Order No. 706, stated that NERC should look to NIST as a source for improving the CIP Reliability Standards. *Id.* P 4.

Document Content(s)