182 FERC ¶ 61,155
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Willie L. Phillips, Acting Chairman;
James P. Danly, Allison Clements,
and Mark C. Christie.

North American Electric Reliability Corporation Docket No. RD23-3-000

ORDER APPROVING RELIABILITY STANDARD CIP-003-9

(Issued March 16, 2023)

1. On December 6, 2022, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted a petition seeking approval of proposed Reliability Standard CIP-003-9 (Cyber Security – Security Management Controls).[1] As discussed in this order, pursuant to section 215(d)(2) of the Federal Power Act (FPA), we approve proposed Reliability Standard CIP-003-9, the associated violation risk factors and violation severity levels, the proposed implementation plan, and the retirement of the currently effective Reliability Standard CIP-003-8 immediately prior to the effective date of the proposed Reliability Standard CIP-003-9.[2] As discussed in this order, we determine that proposed Reliability Standard CIP-003-9 improves upon the currently effective Reliability Standard CIP-003-8 by adding new requirements focused on supply chain risk management for low impact bulk electric system (BES) Cyber Systems.[3]

[1] The proposed Reliability Standard is not attached to this order. The proposed Reliability Standard is available on the Commission's eLibrary document retrieval system in Docket No. RD23-3-000 and on the NERC website, www.nerc.com. We are concurrently issuing a notice of information collection and request for comments in this docket.

[2] 16 U.S.C. § 824o(d)(2).

[3] *See* NERC, *Glossary of Terms Used in NERC Reliability Standards* (Dec. 2, 2022), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (defining BES Cyber System to mean "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity").

I. Background

A. Section 215 and Mandatory Reliability Standards

2. Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[4] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[5] and subsequently certified NERC.[6]

B. NERC Petition and Proposed Reliability Standard CIP-003-9

3. On December 6, 2022, NERC submitted a petition seeking approval of proposed Reliability Standard CIP-003-9. NERC also requested that the Commission approve the associated violation risk factors and violation severity levels, the proposed implementation plan, and the retirement of the currently effective Reliability Standard CIP-003-8 immediately prior to the effective date of the revised Reliability Standard. NERC states that proposed Reliability Standard CIP-003-9 improves upon Commission approved Reliability Standard CIP-003-8 by adding new requirements that focus on supply chain risk management for low impact BES Cyber Systems and enhanced reliability controls that grant responsible entities additional visibility into threats.[7]

4. NERC explains that the proposed modifications stem from recommendations of the 2019 NERC Supply Chain Risk Assessment.[8] Consistent with the findings of the

---

[4] 16 U.S.C. § 824o.

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

[6] *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 clarification and reh'g*, 119 FERC ¶ 61,046 (2007), a*ff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[7] NERC Petition at 4.

[8] *Id.* at Ex. E-2, NERC, *Supply Chain Risk Assessment: Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request* (Dec. 9, 2019), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf (2019 NERC Supply Chain Risk Assessment).

2019 NERC Supply Chain Risk Assessment and directives of the NERC Board of Trustees (NERC Board), the proposed Reliability Standard CIP-003-9 would: (1) require responsible entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies and (2) require responsible entities with assets containing low impact BES Cyber Systems to have methods for determining and disabling vendor electronic remote access.[9]

5. NERC states that when the NERC Board adopted the initial supply chain Reliability Standards applicable to medium and high impact BES Cyber Systems in 2017,[10] it concurrently directed further study of supply chain risks associated with low impact BES Cyber Systems. Pursuant to that directive, NERC asserts that it identified supply chain risks affecting low impact BES Cyber Systems similar to those affecting medium and high impact BES Cyber Systems, such as the introduction of malicious code in the supply chain and remote access of vendors' employees. NERC states that assets associated with low impact BES Cyber Systems pose a lower risk to the bulk electric system if compromised than assets associated with medium or high impact BES Cyber Systems. However, NERC observed that there is the potential for a greater impact if multiple low impact assets are simultaneously compromised through remote access or if a medium or high impact asset is accessed through a low impact asset.[11]

6. The 2019 NERC Supply Chain Risk Assessment reported that most low impact assets are contained in organizations with higher impact assets, although the low impact assets may not receive the same protections, particularly if the low impact assets use separate vendors.[12] The 2019 NERC Supply Chain Risk Assessment further stated that the risk of a coordinated attack on multiple low impact assets with remote electronic access connectivity could result in an event with interconnection-wide impact on the bulk electric system.[13] The 2019 NERC Supply Chain Risk Assessment recommended modification of the Critical Infrastructure Protection (CIP) Reliability Standards to apply

---

[9] *Id.* at 10.

[10] NERC defines the original supply chain Reliability Standards to include Reliability Standards CIP-005-6 (Cyber Security — Electronic Security Perimeter(s)), CIP-010-3 (Cyber Security — Configuration Change Management and Vulnerability Assessments), and CIP-013-1 (Cyber Security - Supply Chain Risk Management). *See Supply Chain Risk Mgmt. Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018).

[11] NERC Petition at 8.

[12] 2019 NERC Supply Chain Risk Assessment at 12.

[13] *Id.*

supply chain risk management requirements to low impact BES Cyber Systems with remote access connectivity.[14]

7. Consistent with the 2019 NERC Supply Chain Risk Assessment, NERC proposes new Requirement R1.2.6 that would require responsible entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies and redesignate the currently effective Requirement R1.2.6 as Requirement R1.2.7.[15] NERC also proposes to modify Attachment 1, section 6 to require 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 vendor electronic remote access.[16]

8. NERC explains that the controls in proposed Attachment 1, section 6 seek to limit the ability to leverage trusted vendor access through supply chain vulnerabilities. Proposed 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. Proposed section 6.2 requires responsible entities to have one or more methods for disabling vendor electronic remote access. Requiring responsible entities to have such a method is intended to prevent propagation of any further issues caused by vendor electronic remote access. 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. The control provides additional visibility to responsible entities in identifying threats and is consistent with the recommendations of the NERC staff.[17]

9. NERC proposes an implementation plan that provides that proposed Reliability Standard CIP-003-9 would become effective on the first day of the first calendar quarter that is 36 months after Commission approval and that the currently effective Reliability Standard CIP-003-8 would be retired immediately prior to the effective date of proposed Reliability Standard CIP-003-9.[18] NERC states that the proposed implementation plan reflects the consideration that there are a large number of low impact BES Cyber Systems

---

[14] *Id.*

[15] NERC Petition at 10.

[16] *Id.* at 11.

[17] *Id.* at 11, 12 (citing Exh. E-1, NERC, *Cyber Security Supply Chain Risks* (May 17, 2019); 2019 NERC Supply Chain Risk Assessment.

[18] NERC Petition at 14.

and responsible entities need time to procure and install equipment that may be subject to delays given high demand.[19] Finally, NERC proposes modifications to the associated violation severity levels of proposed Reliability Standard CIP-003-9, Requirements R1 and R2. For Requirement R1, the modifications to the violation severity level reference the addition of new Requirement 1.2.6. For Requirement R2, the modifications to the violation severity level reference the new policy topic in Attachment 1, Section 6 "vendor electronic remote access security controls."

II. Notice of Filing and Responsive Pleadings

10. Notice of NERC's filing was published in the *Federal Register*, 87 Fed. Reg. 78,680 (Dec. 22, 2022), with interventions and protests due on or before January 5, 2023.

11. The American Public Power Association filed a timely motion to intervene. No protests or comments were received.

III. Procedural Matters

12. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2022), the timely, unopposed motion to intervene serves to make the entity that filed it a party to this proceeding.

IV. Determination

13. Pursuant to section 215(d)(2) of the FPA, we approve Reliability Standard CIP-003-9 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We conclude that Reliability Standard CIP-003-9 is an improvement over the currently effective Reliability Standard CIP-003-8 and will enhance existing protections for reliable operation of the Bulk-Power System by addressing supply chain risks for low impact BES Cyber Systems.

14. Specifically, we determine that Reliability Standard CIP-003-9 improves upon Reliability Standard CIP-003-8 by adding new requirements focused on supply chain risk management for low impact BES Cyber Systems and enhancing reliability controls that grant responsible entities additional visibility into threats. In particular, Reliability Standard CIP-003-9 would do so by: (1) requiring responsible entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies, (2) requiring responsible entities with assets containing low impact BES Cyber Systems to have methods for determining and disabling vendor electronic remote access, and (3) requiring responsible entities with assets containing low impact BES Cyber

[19] *Id.*

Systems to have methods for detecting malicious communications for vendor electronic remote access.

15. We also approve the implementation plan. We agree that the proposed implementation plan reflects consideration that there are a large number of low impact BES Cyber Systems and that responsible entities need time to procure and install equipment that may be subject to delays given high demand. Therefore, we find that the implementation plan strikes an appropriate balance between the urgency to implement Reliability Standard CIP-003-9, the high number of assets containing low impact BES Cyber Systems, and supply chain constraints for equipment necessary to implement the Reliability Standard. In addition, we approve the associated violation risk factors and violation severity level assignments for Reliability StandardCIP-003-9.

16. Finally, we approve the retirement of the currently effective Commission-approved Reliability Standard CIP-003-8 immediately prior to the effective date of Reliability Standard CIP-003-9.

The Commission orders:

The Commission hereby approves: (1) Reliability Standard CIP-003-9, (2) the associated implementation plan, the associated violation risk factors and violation severity levels, and (3) the retirement of the currently effective Commission-approved Reliability Standard CIP-003-8 immediately prior to the effective date of Reliability Standard CIP-003-9, as discussed in the body of this order.

By the Commission.

(S E A L)

Debbie-Anne A. Reese,
Deputy Secretary.