174 FERC ¶ 61,193
FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

March 18, 2021

In Reply Refer To:
North American Electric Reliability Corporation
Docket No. RD21-2-000

North American Electric Reliability Corporation
1325 G Street, NW
Suite 600
Washington, DC 20005

Attention: Lauren Perotti
Marisa Hecht

Dear Ms. Perotti and Ms. Hecht:

1. On December 14, 2020, the North American Electric Reliability Corporation (NERC) filed a petition requesting approval of proposed Reliability Standards CIP-013-2 (Cyber Security – Supply Chain Risk Management), CIP-005-7 (Cyber Security – Electronic Security Perimeter(s)), and CIP-010-4 (Cyber Security – Configuration Change Management and Vulnerability Assessments). NERC also requested approval of: (1) the associated implementation plan, violation risk factors and violation severity levels; and (2) the retirement of currently-effective Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3.[1] For the reasons discussed below, we grant the requested approvals.

2. In Order No. 850, the Commission approved supply chain risk management Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 (Supply Chain Standards), finding that the requirements are forward-looking and objective-based and 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

[1] NERC Petition at 1-2.

associated with bulk electric system operations.[2] While approving the Supply Chain Standards, the Commission determined that a significant cybersecurity risk associated with the supply chain for BES Cyber Systems remained because the approved Reliability Standards did not address Electronic Access Control or Monitoring Systems (EACMS).[3] To address this reliability gap, pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directed NERC to develop and submit modifications to include EACMS in the supply chain risk management Reliability Standards and to file the modifications within 24 months of the effective date of Order No. 850.[4]

3. The Commission also determined that NERC's proposal did not address Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA),[5] with the exception of the modifications in Reliability Standard CIP-005-6, which apply to PCAs, and expressed concerns that the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.[6] The Commission accepted NERC's commitment to evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC Board of Trustees (BOT) in its resolutions of August 10, 2017. The Commission further

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

[3] *Id.* P 4. EACMS are defined as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." North American Electric Reliability Corporation, *Glossary of Terms Used in NERC Reliability Standards* (Jan. 4, 2021) (NERC Glossary).

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

[5] The NERC Glossary defines PACS as "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." NERC defines PCAs as "[o]ne 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. …"

[6] Order No. 850, 165 FERC ¶ 61,020 at P 6.

directed NERC to file the BOT-directed final report with the Commission upon its completion.[7]

4. In response to the BOT directive, NERC states that it evaluated the supply chain risks associated with certain categories of assets not subject to the Supply Chain Standards approved in Order No. 850 and developed a report that included recommended actions to address the identified risks.[8] NERC filed the Supply Chain Report with the Commission, which recommended: (1) revising the Supply Chain Standards to address EACMS that provide electronic access control (excluding monitoring and logging) to high and medium impact bulk electric system (BES) Cyber Systems; and (2) revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.[9]

5. In its petition, NERC submits that the proposed Reliability Standards improve bulk electric system reliability and address the Commission's directive from Order No. 850 as well as the recommendations of the Supply Chain Report.[10] Specifically, proposed Reliability Standard CIP-013-2 requires responsible entities to consider and address cyber security risks from vendor products or services during planning for the procurement of BES Cyber Systems as well as EACMS and PACS. NERC explains that its proposal only includes modifications to Requirement R1, although the entire Reliability Standard applies to EACMS and PACS.[11] Among other things, Requirement R1 requires responsible entities to add EACMS and PACS associated with medium and high impact BES Cyber Systems to their documented supply chain cyber security risk management plans. According to NERC, the proposed modifications address risks during the planning stage when responsible entities are procuring BES Cyber Systems, EACMS, and PACS.[12]

6. NERC further explains that proposed Reliability Standard CIP-005-7 includes requirements that address supply chain risk management in the operational phase.

---

[7] *Id*.

[8] North American Electric Reliability Corporation, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, Docket No. RM17-13-000, at 2 (May 28, 2019) (Supply Chain Report).

[9] *Id*.

[10] NERC Petition at 1-2.

[11] *Id*. at 9.

[12] *Id*. at 9-10.

Requirement R3 includes new Parts 3.1 and 3.2 and addresses remote access controls for EACMS and PACS associated with high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity.[13] NERC asserts that the new provisions work in tandem with Requirement R1, Part 1.2.6 of proposed Reliability Standard CIP-013-2 to address vendor remote access and are similar to Reliability Standard CIP-005-7, Requirement R2, Parts 2.4 and 2.5, which address remote access controls in the operational phase for medium and high impact BES Cyber Systems.[14]

7. As proposed by NERC, the revised language of Reliability Standard CIP-010-4 expands applicability to EACMS associated with high and medium impact BES Cyber Systems, and PACS associated with high and medium impact BES Cyber Systems.[15] NERC explains that the revised Reliability Standard will now help reduce the risk of an attacker exploiting a legitimate vendor patch management process for EACMS and PACS by requiring responsible entities to apply these protections to EACMS and PACS.[16]

8. Notice of NERC's December 14, 2020 filing was published in the *Federal Register*, 86 FR 2668 (2021), with interventions and protests due on or before January 28, 2021. No interventions or comments were received.

9. Pursuant to section 215(d)(2) of the FPA, we approve Reliability Standards CIP-013-2, CIP-005-7 and CIP-010-4, their associated implementation plan, violation risk factors and violation severity levels.[17] We determine that the proposed Reliability Standards satisfy the directive in Order No. 850 to modify these Reliability Standards to include EACMS as applicable systems. The proposed Reliability Standards also address

[13] *Id*. at 11.

[14] *Id*. at 12.

[15] *Id*. at 13.

[16] *Id*. at 14.

[17] 16 U.S.C. § 824o(d)(2). In compliance with the requirements of the Paperwork Reduction Act of 1995, 44 USC 3506(c)(2)(A), the Commission issued a *Notice of Information Collection and Request for Comments* on February 22, 2020.

the Commission's concern that the exclusion of PACS may leave a gap in the supply chain risk management Reliability Standards.

By direction of the Commission.

Kimberly D. Bose,
Secretary.