6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. RM20-12-000]

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards

AGENCY: Federal Energy Regulatory Commission.

ACTION: Withdrawal of notice of inquiry and termination of rulemaking proceeding.

SUMMARY: The Commission withdraws a notice of inquiry, which sought comment on whether the then-effective Critical Infrastructure Protection (CIP) Reliability Standards adequately addressed: cybersecurity risks pertaining to data security, detection of anomalies and events, and mitigation of cybersecurity events. The Commission also sought comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether Commission action, including potential modifications to the CIP Reliability Standards, would be appropriate to address such risk.

DATES: This withdrawal will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

FOR FURTHER INFORMATION CONTACT:

Leigh Anne Faugust

Office of the General Counsel

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

(202) 502-6396

leigh.faugust@ferc.gov

SUPPLEMENTARY INFORMATION:

1. On June 18, 2020, the Commission issued a notice of inquiry in this proceeding. The notice of inquiry sought comment on potential enhancements to the Critical Infrastructure Protection (CIP) Reliability Standards corresponding to certain aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST Framework) and the risk of coordinated cyberattack to the security and reliability of the Bulk-Power System.[1]

2. As set forth below, we exercise our discretion to withdraw the notice of inquiry and terminate this rulemaking proceeding.

I. Background

3. In the notice of inquiry, the Commission sought comment on whether the then-effective CIP Reliability Standards adequately addressed the following topics: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events. Commission staff identified these topics after reviewing the NIST Framework and comparing its content to that of the CIP Reliability Standards. The Commission also sought comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether Commission action, including potential modifications to the CIP Reliability Standards, would be

[1] *Potential Enhancements to the Critical Infrastructure Prot. Reliability Standards*, Notice of Inquiry, 171 FERC ¶ 61,215 (June 18, 2020) (Notice of Inquiry); NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

proper to address such risk. In issuing the notice of inquiry, the Commission explained that as "new cyber threats continue to evolve, the Reliability Standards should keep pace to support a robust, defense in depth approach to electric grid cybersecurity."[2]

A. Comments

4. The Commission received 24 comments in response to the questions posed in the notice of inquiry.[3] Most commenters responded that the then-effective Reliability Standards, together with Reliability Standards pending implementation and Reliability Standards under development by NERC at that time, adequately addressed the NIST Framework categories identified in the notice of inquiry.[4] Other commenters acknowledged that the Reliability Standards may not address some aspects of the NIST Framework but asserted that the NIST Framework and CIP Reliability Standards serve fundamentally different purposes and, as a result, cautioned against an apples-to-apples

---

[2] Notice of Inquiry, 171 FERC ¶ 62,215 at P 2.

[3] Comments were received from: jointly, American Public Power Association (APPA) and Large Public Power Council (LPPC); Jonathan Appelbaum (Appelbaum); Canadian Electricity Association; Cogentrix Energy Power Management, LLC; Jason Christopher and Tim Conway (Christopher and Conway); George R. Cotter; Jointly, Edison Electric Institute (EEI) and Electric Power Supply Association (EPSA); Forescout Technologies, Inc. (Forescout); Independent System Operators and Regional Transmission Organizations Council (IRC); National Rural Electric Cooperative Association; New Jersey Board of Public Utilities (NJ PUC); North American Electric Reliability Corporation (NERC); MISO Transmission Owners (MISO TO); Reliable Energy Analytics, LLC (REA); Siemens Energy, Inc.; Solar Energy Industries Association (SEIA); Southern Company Services, Inc. for Southern Power Co., Mississippi Power Co., Georgia Power Co., and Alabama Power Co.; Southwestern Power Administration; Transmission Access Policy Study Group; United States Army Corps of Engineers; United States Bureau of Reclamation; Western Area Power Administration; Wolverine Power Supply Cooperative, Inc.; and XTec, Inc.

[4] *See e.g.,* NERC Comments at 7; EEI and EPSA Comments at 8-10; MISO TOs Comments at 5-6; IRC Comments at 2-3.

comparison of the two regimes.[5] Some commenters did identify potential areas for improvement.[6]

5. Regarding coordinated cyberattacks, the comments identified Reliability Standards, NERC programs, and voluntary actions that industry was taking to address the potential risk.[7] Other commenters suggested that there should be additional protections for low impact bulk electric system (BES) Cyber Systems.[8]

II. Discussion

6. We appreciate the feedback that the Commission received in response to the notice of inquiry. After careful consideration of the record, including later actions by NERC and the Commission to address issues core to the notice of inquiry, we exercise our discretion to withdraw the notice of inquiry and terminate this proceeding.[9]

7. After the issuance of the notice of inquiry, NERC and the Commission took multiple actions to address emerging issues and to improve the cybersecurity posture of the BES. For example, the Commission addressed control center communication by

---

[5] *See, e.g.,* EEI/EPSA Comments at 4; APPA and LPPC Comments at 1-2; Christopher and Conway Comments at 6. Other comments support the use of the NIST Framework as a reference. *See, e.g.,* NJ PUC Comments at 3.

[6] *See e.g.,* REA Comments at 3-4; Appelbaum Comments at 9, 16.

[7] *See* NERC Comments at 16 (explaining it could mitigate the risks of coordinated cyberattacks through: (1) assessments, reports, and studies; (2) alerts and lessons learned issuances; (3) collaboration on risk prioritization with stakeholders; (4) information sharing; and (5) simulated training exercises); *see also* SEIA Comments at 6; EEI and EPSA Comments at 14-15; MISO TO Comments at 8-9.

[8] *See e.g.,* Applebaum Comments at 25; Forescout Comments at 1-2.

[9] *See, e.g.*, *Revised Pub. Util. Filing Requirements for Elec. Quarterly Reps.,* 169 FERC ¶ 61,236 (2019) (order withdrawing notice of proposed rulemaking and terminating rulemaking proceeding); *see also, e.g.*, *Fast-Start Pricing in Mkts. Operated by Reg'l Transmission Org. & Indep. Sys. Operators,* 161 FERC ¶ 61,293 (2017) (order withdrawing notice of proposed rulemaking and terminating rulemaking proceeding).

approving Reliability Standard CIP-012-1 (Communications Between Control Centers) in 2020 in Order No. 866 and directing NERC to develop modifications to the CIP Reliability Standards to require protections regarding the availability of communication links and data communicated (specifically the confidentiality and integrity of Real-time Assessment and Real-time monitoring data) between control centers.[10] NERC developed responsive modifications and the Commission then approved the revised Standard on May 23, 2024.[11]

8. The Commission also took steps to improve the detection of anomalies and detection and mitigation of cybersecurity events. Specifically, on January 19, 2023, the Commission issued Order No. 887 directing NERC to develop requirements for internal network security monitoring, which NERC submitted on June 24, 2024. Concurrently with this proceeding, we are approving Reliability Standard CIP-015-1 (Internal Network Security Monitoring) and directing further improvements to the Standard.[12]

9. Regarding the potential risk of a coordinated cyberattack on geographically distributed targets, on March 16, 2023, the Commission approved Reliability Standard CIP-003-9 (Security Management Controls).[13] The Standard requires entities with BES facilities whose assets are designated low impact to have methods for determining and disabling vendor remote access. NERC also performed an in-depth analysis of the risk

---

[10] *Critical Infrastructure Prot. Reliability Standard CIP-012-1 – Cyber Sec. – Communic's between Control Ctrs.*, Order No. 866, 85 FR 7197 (Feb. 7, 2020), 170 FERC ¶ 61,031, at P 36 (2020).

[11] *N. Am. Elec. Reliability Corp.,* 187 FERC ¶ 61,086 (2024).

[12] *Critical Infrastructure Prot. Reliability Standard CIP-015-1 – Cyber Sec. – Internal Network Sec. Monitoring*, 191 FERC ¶ 61,224 (2025).

[13] *N. Am. Elec. Reliability Corp.,* 182 FERC ¶ 61,155 (2023).

presented by low impact cyber facilities and reported on whether those criteria should be modified to address coordinated cyberattacks.[14] Based on those findings, NERC revised Reliability Standard CIP-003 and, on December 20, 2024, NERC filed proposed Reliability Standard CIP-003-11 (Security Management Controls) for Commission approval.[15] The proposed Standard would, among other things, require entities to "mitigate the risks posed by a coordinated attack using distributed low impact bulk electric system Cyber Systems by adding controls to authenticate remote users; protecting the authentication information in transit; and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity."[16]

The Commission orders:

The notice of inquiry is hereby withdrawn and Docket No. RM20-12-000 is hereby terminated.

By the Commission. Commissioner Chang is not participating.

Issued: June 26, 2025.

Carlos D. Clay,

---

[14] *Minutes: Board of Trustees*, 7 (Feb. 4, 2021), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Feb%204%202021.pdf.

[15] *N. Am. Elec. Reliability Corp.,* Petition for Approval of Proposed Reliability Standard CIP-003-11, Docket No. RM25-8-000 (filed Dec. 20, 2024) (currently pending before the Commission). Withdrawing the notice of inquiry and terminating this docket does not pre-judge the Commission's action in the pending docket (e.g., whether or not the Commission will approve the proposed Reliability Standard).

[16] *Id.* at 1-2.

Deputy Secretary.

[FR Doc. 2025-12265 Filed: 6/30/2025 8:45 am; Publication Date: 7/1/2025]