UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Critical Infrastructure Protection Reliability Standard CIP-015-10 – Cybersecurity – Internal Network Security Monitoring	)))	Docket No. RM24-7-000

COMMENTS OF THE NEW ENGLAND STATES COMMITTEE ON ELECTRICITY

Pursuant to the Notice of Proposed Rulemaking issued by the Federal Energy Regulatory Commission ("Commission" or "FERC") on September 19, 2024,[1] the New England States Committee on Electricity ("NESCOE") files comments on the Commission's proposal to approve proposed Critical Infrastructure Protection ("CIP") Reliability Standard CIP-015-1 (Cyber Security – Internal Network Security Monitoring) as well as the Commission's proposal to direct that the North American Electric Reliability Corporation ("NERC") develop further modifications to reliability standard CIP-015-1 to extend Internal Network Security Monitoring ("INSM") to include electronic access control or monitoring systems ("EACMS") and physical access control systems ("PACS") outside of the electronic security perimeter.[2]

I. DESCRIPTION OF COMMENTER

NESCOE is the Regional State Committee ("RSC") for New England. It is governed by a board of managers appointed by the Governors of Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont and is funded through a regional tariff that ISO New

---

1 *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring*, 188 FERC ¶ 61,175 (2024) ("NOPR").

2 NOPR at P 1.

England Inc. ("ISO-NE") administers.[3] NESCOE's mission is to represent the interests of the citizens of the New England region by advancing policies that will provide electricity at the lowest possible price over the long term, consistent with maintaining reliable service and environmental quality.[4] These comments represent the collective view of the six New England States.

II. COMMENTS

NESCOE strongly supports efforts to ensure cybersecurity reliability[5] and appreciates the Commission's efforts to improve the cybersecurity posture of the Bulk-Power System.

Cybersecurity is a critical facet of the Bulk-Power System's reliability and resilience.[6] In New England and across the country, grid transformation is expanding the potential for cyberattacks due to the use of emerging technologies, additional communications, and industrial controls as well as remote control capabilities.[7] While these technologies can offer a wide range of benefits, they can also pose emerging cybersecurity challenges for the electric grid.[8] For

---

3 *ISO New England Inc.*, 121 FERC ¶ 61,105 (2007).

4 *See* Sept. 8, 2006 NESCOE Term Sheet ("Term Sheet") that was filed for information as Exhibit A to the Memorandum of Understanding among ISO-NE, the New England Power Pool ("NEPOOL"), and NESCOE (the "NESCOE MOU"). Informational Filing of the New England States Committee on Electricity, Docket No. ER07-1324-000 (filed Nov. 21, 2007). Pursuant to the NESCOE MOU, the Term Sheet is the binding obligation of ISO-NE, NEPOOL, and NESCOE.

5 *Cross Sound Cable Company, LLC*, Protest of the New England States Committee on Electricity, Docket No. ER21-2334-000 (July 22, 2021), at 6, at https://nescoe.com/wp-content/uploads/2021/07/Protest_ER21-2334_7-22-21.pdf.

6 North American Electric Reliability Corporation, Quick Reference Guide: Security Integration (Apr. 2024), at 1, available at https://www.nerc.com/pa/Documents/Security_Integration__Quick_Reference_Guide.pdf.

7 North American Electric Reliability Corporation, Quick Reference Guide: Security Integration (Apr. 2024), at 1, available at https://www.nerc.com/pa/Documents/Security_Integration__Quick_Reference_Guide.pdf.

8 *See, e.g.*, U.S. Department of Energy, *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid* (Oct. 2022), available at https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf.

example, software and hardware used across the electric industry[9] can be targeted by hackers via direct network attacks or supply chain breaches.[10] Accordingly, it is more important than ever that the Commission take all necessary steps to make sure that malicious actors cannot threaten the security of our electric grid. This, in turn, will help enable the adoption of new grid technologies in a way that bolsters both performance and reliability.

The Commission's proposals are aimed at closing a reliability and security gap that would otherwise potentially allow malicious actors to target the electric grid.[11] Accordingly, NESCOE supports the NOPR proposals and encourages the continued efforts of the Commission to ensure the cybersecurity of the bulk-power system.

III. CONCLUSION

NESCOE thanks the Commission for its consideration of these Comments.

---

[9] *See*, *e.g.*, SolarWinds and Related Supply Chain Compromise at 8, 10-16, available at https://cms.ferc.gov/media/solarwinds-and-related-supply-chain-compromise-0.

[10] A supply chain attack works by targeting a third party with access to an organization's systems. The Commission has pointed to the SolarWinds attack as an example of how an attacker can bypass all network perimeter-based security controls traditionally used to identify the early phases of an attack. *See Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, 182 FERC ¶ 61,021, at P 15 (2023) (Order No. 887) (citing *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys., Notice of Proposed Rulemaking*, 178 FERC ¶ 61,038, at P (2022) (internal citations omitted); *see also* SolarWinds and Related Supply Chain Compromise at 10-16, available at https://cms.ferc.gov/media/solarwinds-and-related-supply-chain-compromise-0.

[11] NOPR at P 11.

Respectfully Submitted,

/s/ Shannon Beale

Shannon Beale
Assistant General Counsel
New England States Committee on Electricity
P.O. Box 322
Osterville, MA 02655
Tel: (781) 400-9000
Email: shannonbeale@nescoe.com

Dated: November 26, 2024