UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Incentives for Advanced Cybersecurity Investment	**)** **)**	**Docket No. RM22-19-000**

JOINT COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION AND THE REGIONAL ENTITIES IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") and the six Regional Entities,[1] collectively the "Electric Reliability Organization ("ERO") Enterprise," submit comments on the Federal Energy Regulatory Commission ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR") regarding incentive-based rate treatments for voluntary cybersecurity investments.[2] Specifically, the Commission seeks comment on (1) the proposed eligibility criteria and approaches to evaluate eligibility for the proposed rate incentives; (2) the proposed rate incentives; and (3) the time limit for receiving incentives.

The ERO Enterprise supports continued efforts to strengthen the cybersecurity posture of registered entities and other industry stakeholders to enhance the reliability and security of the Bulk Power System ("BPS"). The ERO Enterprise appreciates the Commission considering a variety of methods to encourage entities to enhance their cybersecurity posture and invest in cybersecurity. The ERO Enterprise requests that the Commission consider in its final rule the relationship between rate incentives for cybersecurity investments and compliance with NERC's Critical Infrastructure Protection ("CIP") Reliability Standards.

---

[1] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

[2] *Incentives for Advanced Cybersecurity Investment*, Notice of Proposed Rulemaking; Notice Terminating Proceeding, 180 FERC ¶ 61,189 (2022) [hereinafter NOPR].

I. COMMENTS

A. The ERO Enterprise supports Commission efforts to encourage industry to strengthen cybersecurity practices

As the Commission discusses in the NOPR, it is important to consider or employ various methods to encourage strong cybersecurity practices through a defense-in-depth approach. As noted in the 2022 NERC State of Reliability Report, the electric industry faced a security threat landscape "that was both unprecedented and relentless."[3] Furthermore, entities increasingly rely on digital information and microprocessor-driven devices to maintain operations.[4] The combination of unprecedented threats and increased reliance on programmable technology to operate the BPS demonstrates that security is necessary for reliability and resilience.

As noted in Jim Robb's testimony to the Senate Energy Committee in 2019:[5]

> The security landscape is dynamic, requiring constant vigilance and agility. NERC assures grid security through a comprehensive series of complementary strategies involving mandatory standards, information sharing, and partnerships. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections.
>
> Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit both within the North American electricity industry and between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to determine and maintain "ground truth" during rapidly evolving security events. The E-ISAC also plays a key role in cross-sector coordination, focusing on sectors with which electricity has interdependencies, such as natural gas, water, and other critical infrastructure. Mandatory standards, coupled with effective mechanisms to share information, provide robust and flexible tools to protect the BPS.

---

[3] NERC, *State of Reliability Report* at p. 59 (July 2022), https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2022.pdf.

[4] *Id.* at p. 60.

[5] *Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry*, before the Senate Comm. on Energy and Natural Resources, 117th Cong. (Feb. 14, 2019) (Statement of James B. Robb, President and Chief Executive Officer, North American Electric Reliability Corporation), https://www.nerc.com/news/testimony/Testimony%20and%20Speeches/Senate%20Energy%20Committee%20Cyber%20Hearing%20Testimony%20February%2014%202019.pdf.

Continued investment in cybersecurity is crucial to maintaining the reliable operation of the BPS. While the ERO Enterprise does not take a position on the necessity, amount, duration, or type of rate incentives, the ERO Enterprise appreciates the Commission's consideration of the need for additional cybersecurity investments to help ensure BPS reliability and security. Along those lines, NERC has organized a team of cyber engineering experts who are working with the various working groups and subcommittees reporting to the Reliability and Security Technical Committee ("RSTC") to provide guidance on robust cyber system and process design:

- **Managing Current Cyber Risk and Emerging Grid Transformation:** The integration of large amounts of inverter-based resources can broaden the potential for an increased cyber threat surface. Planning, engineering, design, and operations need to ensure that cybersecurity is not addressed after the fact, but part of the system design.
- **Guideline Development:** NERC has RSTC-approved guidelines that include, but are not limited to, Open Source Software, Risk Management Life Cycle, Supply Chains, and Cloud Computing. Work continues on guidelines on supply chain management and distributed energy aggregators.

NERC CIP Reliability Standards have undergone a transformation over the past several years and continue to progress based on experience with the standards and evolving understanding of risk. Beginning with implementation of the CIP Version 5 standards in 2016, entities have implemented several new requirements that expand security protections.[6] NERC continues to work with industry subject matter experts to revise the CIP Reliability Standards to strengthen their efficacy. Any incentives for voluntary cybersecurity investments should build upon and complement the cybersecurity standards in place.

The ERO Enterprise is pleased that the Commission's NOPR proposal includes CRISP on the pre-qualified list of investments as it recognizes the importance and efficacy of such

[6] The suite of standards referred to as CIP Version 5 include the following standards and their successor versions: CIP-002-5.1a, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1.

information sharing programs. As noted in the NOPR, the E-ISAC administers CRISP, in coordination with the Department of Energy ("DOE") and the Pacific Northwest National Laboratory ("PNNL"). CRISP provides a two-way exchange of unclassified and classified threat information affecting the energy sector. Data shared through the CRISP program is near-real-time, with analysts at DOE and PNNL providing identification of threat patterns and attack indicators across the energy industry. Rate incentives, when necessary to spur investment, could be an appropriate mechanism, among others, to help expand programs like CRISP and, in turn, enhance the information sharing practices across industry to strengthen cyber defenses.

In addition to CRISP, the E-ISAC is actively involved in an operational technology ("OT") visibility program. These sensors were deployed as part of the executive branch's 100-day sprint in spring 2021. The E-ISAC is analyzing data from these sensors and conducting threat hunts. The ERO Enterprise recommends the Commission also include the further deployment of these OT sensors on its list of pre-qualified investments because, as with CRISP, rate incentives, when necessary, could be an appropriate mechanism to help build and enlarge OT visibility programs, particularly among small and medium-sized entities.

B. The Commission should consider the relationship between rate incentives and compliance with the CIP standards

The Commission proposes to exclude from rate incentive "advanced cybersecurity technology or participation in a cybersecurity threat information sharing program" that are "already mandated by the [CIP] Reliability Standards…."[7] As the Commission considers this proposal in its final rule, it must consider the relationship between the manner in which entities demonstrate compliance with the CIP standards and the potential exclusion of investments in security tools that demonstrate compliance from rate incentives. NERC Reliability Standards are

[7] NOPR at P 20.

technology-neutral. CIP requirements do not prescribe a particular technological method, tool, or approach to comply. The CIP Reliability Standards generally provide flexibility in how registered entities identify, categorize, protect, and monitor applicable BES Cyber Systems; there is no one "mandated" technology for compliance with CIP Reliability Standards.

As such, an entity could use any number of approaches to comply with a particular requirement. In practice, the ERO Enterprise has found that entities often employ a defense-in-depth approach to compliance, using multiple approaches and tools to comply with a single standard. As relevant to this NOPR, to comply with the requirements CIP-007-6, Requirement R3, Part 3.1 and CIP-005-7, Requirement R1, Part 1.5 to detect malicious code and malicious communications, registered entities could use internal network security monitoring tools in combination with other tools and processes.

Given that there is no single investment mandated by the CIP standards and registered entities often use a number of methods to meet a single requirement, it may be a challenge for entities and the Commission to determine whether a particular investment is "mandated" by the CIP standards and should thus be excluded from rate incentives. As in the circumstance noted above, while not specifically mandated or absolutely necessary for compliance, one of the investments an entity may use to help demonstrate compliance with CIP-007-6, Requirement R3, Part 3.1 and CIP-005-7, Requirement R1, Part 1.5 is an internal network security monitoring tool that is also included on the pre-qualified list for rate incentives. In its final rule, the Commission should articulate how and whether it would grant incentives for investments on the pre-qualified list that, while not mandated by the CIP standards, help an entity demonstrate compliance with those standards.

Finally, the Commission should consider the relationship between the ongoing revisions to the CIP Reliability Standards and the eligible investments in the final rule. Industry stakeholders should not be discouraged from making necessary revisions to the existing CIP Reliability Standards due to possibly losing the incentive prior to the expiration of the full term of the investments' eligibility.

II. CONCLUSION

The ERO Enterprise appreciates the opportunity to comment in this matter. As discussed above, the ERO Enterprise supports the Commission exploring ways to encourage entities to invest in cybersecurity. The ERO Enterprise also requests that the Commission consider potential impacts on the tools entities use to demonstrate compliance.

Respectfully submitted,

/s/ Marisa Hecht

/s/ Niki Schaefer
Niki Schaefer
Vice President & General Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, Ohio 44131
(216) 503-0600
(216) 503-9207 - facsimile
niki.schaefer@rfirst.org
Counsel for ReliabilityFirst Corporation

/s/ Holly A. Hawkins
Holly A. Hawkins
Vice President, General Counsel, and Corporate Secretary
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 357-7372
hhawkins@serc1.org
Counsel for the SERC Reliability Corporation

Shamai Elstein
Associate General Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net
Counsel for the North American Electric Reliability Corporation

/s/ Lisa A. Zell
Lisa A. Zell
Vice President General Counsel and Corporate Secretary
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1760

/s/ Derrick Davis
Derrick Davis
General Counsel & Corporate Secretary
Texas Reliability Entity, Inc.
805 Las Cimas Parkway, Suite 200
Austin, TX 78746
(512) 583-4900
derrick.davis@texasre.org
Counsel for Texas Reliability Entity, Inc.

/s/ Jeff Droubay
Jeff Droubay
Vice President and General Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6879
jdroubay@wecc.org
Counsel for the Western Electricity Coordinating Council

Date: November 7, 2022

lisa.zell@mro.net
Counsel for Midwest Reliability Organization

/s/ Damase Hebert
Damase Hebert
Associate General Counsel & Director, Enforcement
Northeast Power Coordinating Council, Inc.
1040 Ave. of the Americas, 10th Floor
New York, NY 10018
(212) 840-1070
dhebert@npcc.org
Counsel for Northeast Power Coordinating Council, Inc.