UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	**)**	**Docket No. RM21-3-000**

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 proposed revisions to its regulations to establish rules for incentive-based rate treatments for voluntary cybersecurity investments for a public utility for or in connection with the transmission or sale of electric energy subject to the jurisdiction of the Commission.[2] Specifically, the Commission seeks comment on two approaches to granting these incentives: (1) voluntarily applying a higher level of the Critical Infrastructure Protection ("CIP") Reliability Standards;[3] or (2) implementing certain security controls included in the National Institute of Standards and Technology ("NIST") Framework.

The ERO Enterprise supports continued efforts to strengthen the cybersecurity posture of Responsible Entities[4] and other industry stakeholders to enhance reliability. As such, the ERO Enterprise appreciates the Commission considering a variety of methods to encourage Responsible

---

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

[2] *Cybersecurity Incentives,* Notice of Proposed Rulemaking, 173 FERC ¶ 61,240 (2020) [hereinafter NOPR].

[3] As noted in the NOPR, the CIP Reliability Standards "implement a tiered approach to categorize assets, identifying them as high, medium, or low risk to the operation of the Bulk Electric System ("BES")." NOPR at P 7.

[4] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

Entities to enhance their cybersecurity posture, including seeking comment on the approaches proposed in the NOPR.

The ERO Enterprise submits these comments to focus the Commission's attention on the potential implications for the ERO Enterprise should the Commission adopt the CIP approach in the NOPR. As more fully described in the body of these comments, the ERO Enterprise requests the Commission consider: (1) any role the ERO Enterprise may have in monitoring or reviewing applications and subsequent reports for these incentives; (2) the impact on ERO Enterprise operations; and (3) other details that may impact the ERO Enterprise activities.

These comments are organized into the following sections: Section I.A includes the ERO Enterprise support of the Commission seeking to promote cybersecurity investments; Section I.B urges the Commission to consider the implications for compliance monitoring and enforcement activities; and Section I.C provides the ERO Enterprise comments on the potential impacts to the standards development process. Section II provides a conclusion to these comments.

I. COMMENTS

As noted above, the Commission's NOPR proposes granting incentives for cybersecurity investments. These incentives include the following: (1) an increase in the return on equity applicable to certain cybersecurity investments; (2) deferred cost recovery for certain cybersecurity investments; and (3) other cybersecurity incentives, on a case-by-case basis, if they are just and reasonable and not unduly discriminatory or preferential.[5] Public utilities must apply by filing for Commission approval pursuant to Federal Power Act ("FPA") section 205 and receive such approval prior to implementing the proposed incentives in its Commission-jurisdictional rates and should make annual informational filings thereafter.[6]

[5] NOPR at PP 38-47.

[6] *Id.* at PP 48-49.

In order to receive those incentives, the Commission proposes to follow two approaches to include in applications. The first approach involves demonstrating a voluntary investment in applying the requirements of CIP Reliability Standards that are above and beyond what the entity is required to do. The Commission proposes two ways for a public utility to demonstrate that it is eligible for a cybersecurity incentive under the proposed CIP approach: (1) the medium/high incentive; and (2) the hub-spoke incentive.[7] Under the medium/high incentive, a public utility may receive incentive rate treatment for voluntarily applying requirements for medium or high impact BES Cyber Systems to low impact BES Cyber Systems or by applying the requirements for high impact BES Cyber Systems to medium impact BES Cyber Systems. Under the hub-spoke incentive, a public utility would receive incentive rate treatment for voluntarily ensuring that all routable protocol to and from the low impact BES Cyber System connects to a high or medium impact BES Cyber System. Through this approach, communications to and from the low impact BES Cyber System would inherit the controls applied to the higher impact BES Cyber Systems. These public utilities would receive a rebuttable presumption that the investments materially enhance the public utility's cybersecurity posture.

The second approach involves demonstrating cybersecurity investments that implement security controls from the NIST Framework. The Commission proposes to limit the types of controls to those that are "most likely to provide a significant benefit of Commission-jurisdictional transmission facilities, not just the BES."[8] Entities applying for incentives under the NIST Framework approach must demonstrate that these controls go above and beyond those required by the CIP Reliability Standards.[9]

---

7 *Id.* at PP 22-29.
8 *Id.* at P 33.
9 *Id.* at P 36.

The ERO Enterprise submits the comments below to focus on the implications of the proposed CIP approach to ERO Enterprise activities.

A. The ERO Enterprise supports Commission efforts to encourage industry in strengthening cybersecurity.

The ERO Enterprise agrees with the Commission that it is important to consider or employ various methods to encourage strong cybersecurity practices. To that end, the ERO Enterprise works with entities to voluntarily adopt secure practices, which is consistent with the ERO Enterprise defense-in-depth approach. As noted in the 2020 NERC Annual Report, "[t]he ERO Enterprise has shifted from a primarily compliance-focused approach to one that incorporates a more holistic, risk-based approach in pursuit of continuous improvement, innovation, and value-driven efforts."[10] This shift permits the ERO Enterprise to adeptly address emerging risks. One such focus is on supply chain risk mitigation. The ERO Enterprise has pursued several activities to support entities in this risk mitigation, including NERC alerts, partnerships with the North American Transmission Forum and the Department of Energy, and numerous workshops, such as those hosted by SERC Reliability Corporation and ReliabilityFirst, among others. The ERO Enterprise often collaborates with stakeholder groups to develop best practices. The NERC Supply Chain Working Group, a subgroup of the NERC Reliability and Security Technical Committee ("RSTC"), developed eight reliability guidelines that focused on supply chain security risks. In addition, Regional Entity groups, such as the MRO Security Advisory Council,[11] for example, perform outreach and promote security awareness. These are just a few examples of the ERO

[10] *NERC 2020 Annual Report*, p. 10 (Feb. 2021), https://www.nerc.com/gov/Annual%20Reports/NERC_Annual%20Report_2020.pdf.

[11] The MRO Security Advisory Council is an MRO Organizational Group that provides advice and counsel to MRO's Board of Directors, staff, members, and registered entities regarding: (1) cybersecurity; (2) physical security; and (3) Supervisory Control and Data Acquisition ("SCADA"), Energy Management System ("EMS"), substation and generation control systems.

Enterprise approach to improving the cybersecurity posture of entities through mechanisms above and beyond Reliability Standards alone.

In addition, the ERO Enterprise encourages entities to adopt strong internal controls, including referencing frameworks such as NIST. Recently, ERO Enterprise staff and NIST staff, with contributions from a working group of NERC's RSTC, developed an updated mapping of the currently enforceable CIP Reliability Standards to the NIST Framework.[12] This effort assists entities in understanding how the NIST framework can align with the CIP standards.

Finally, even within compliance monitoring and enforcement activities, the ERO Enterprise assists entities in other ways to strengthen cybersecurity beyond just complying with standards. For example, audit reports include recommendations and positive observations that often highlight areas where security could be improved or areas where the entity has strong controls. Additionally, during enforcement of noncompliance, the ERO Enterprise requires entities to correct the noncompliance and to take steps to reduce the risk of repeat noncompliance.

B. The Commission should consider the implications of the CIP incentives approaches for ERO Enterprise compliance monitoring and enforcement activities prior to adopting the proposed approaches.

Under Section 215(e) of the FPA and Commission regulations implementing the FPA, NERC, as the ERO, has the authority to enforce Reliability Standards.[13] To carry out this authority, the ERO Enterprise developed the Compliance Monitoring and Enforcement Program ("CMEP").[14] This program includes the procedures and processes the ERO Enterprise uses to monitor, assess, and enforce compliance with mandatory Reliability Standards, including the CIP

---

[12] The full mapping is available at https://www.nerc.com/pa/comp/CAOneStopShop/NIST%20CSF%20v1.1%20to%20NERC%20CIP%20FINAL.XLSX.

[13] 16 U.S.C. § 824(o)(e) (2018); 18 C.F.R. § 39 (2020).

[14] NERC, *Rules of Procedure*, Section 400 and Appendix 4C.

standards, in the United States. As such, the ERO Enterprise provides the following comments on considerations for implications for carrying out its statutory and regulatory duty to perform compliance monitoring and enforcement of the CIP Reliability Standards. Section I.B.i. requests consideration of whether there is an ERO Enterprise role in the CIP approach. Section I.B.ii requests consideration of impact on ERO Enterprise operations. Finally, Section I.B.iii presents other considerations for the Commission. NERC respectfully requests that the Commission address these considerations if it determines to adopt its proposed CIP approaches in a final rule issued in this proceeding.

i. Does the ERO Enterprise have a role in monitoring the proposed CIP approach?

The ERO Enterprise has concerns regarding notification of whether an entity had adopted or applies for adoption of voluntary standards under the CIP approach for granting incentives. As such, the ERO Enterprise requests the Commission consider whether the ERO Enterprise will need to evaluate or audit voluntary adoption of requirements or whether the Commission envisions a role for the ERO Enterprise in evaluations. Items to consider include:

(1) whether the ERO Enterprise role would be ongoing and the sustainability of that role;

(2) whether the ERO Enterprise should include monitoring implementation of voluntary standards in its oversight planning;

(3) whether the ERO Enterprise has a role in reviewing the initial application for incentives or any subsequent reports and the sustainability of that role; and

(4) whether the ERO Enterprise should intervene in each proceeding or otherwise be involved in each proceeding and the sustainability of that involvement.

In addition, the ERO Enterprise requests the Commission consider whether it is expected to report any deviations from voluntary adoption of CIP standards for entities receiving incentives

that it discovers during its review of implementation of the mandatory CIP standards. There may be deviations from voluntary application of the CIP requirements, particularly for those entities that have not applied medium and high impact requirements to other BES Cyber Systems. If the ERO Enterprise is expected to report these deviations, it is not clear on when and how the ERO Enterprise should report them.

Likewise, if the Commission is responsible for reviewing compliance with voluntary standards, and there is a non-compliance with the mandatory standards as well, the ERO Enterprise requests consideration of whether the Commission will communicate any potential noncompliance of mandatory standards or any other relevant findings to the ERO Enterprise and how that communication will occur.

ii. Regardless of ERO Enterprise role, what is the impact on ERO Enterprise compliance monitoring and enforcement operations?

The ERO Enterprise requests consideration of whether penalties may still be imposed if an entity also violates mandatory standards while deviating from voluntary standards. The ERO Enterprise asserts that penalties may be imposed, consistent with Section 215 of the FPA, but requests confirmation from the Commission nonetheless. Along those lines, the ERO Enterprise requests consideration of whether it still should consider the voluntarily adopted higher level of controls in penalty assessments if an entity is receiving incentives or whether that would be considered "double credit" for these investments.

To carry out its CMEP activities, the ERO Enterprise employs various tools and mechanisms that may be impacted by this incentives approach. For instance, the Commission should consider the impact on risk-based CMEP tools, such as compliance oversight plans and Inherent Risk Assessments, among others. Actions taken to achieve these incentives likely would impact the output of these tools. As such, the ERO Enterprise needs to consider whether this

information would be expected to be incorporated into these CMEP tools. If the ERO Enterprise is not involved in the evaluation of the application for these incentives, the ERO Enterprise requests consideration of when it would find out entities are taking advantage of these incentives. The ERO Enterprise should be able to factor the information from the incentives applications into these CMEP tools based on timely notification.

iii. How will other considerations relating to confidential information treatment, NERC's intervenor status, and security concerns be addressed?

The ERO Enterprise supports the Commission's proposal to allow public utilities applying for incentive rate treatment to request protection of their information that could lead to the disclosure of confidential information or Critical Energy/Electric Infrastructure Information ("CEII") related to their cybersecurity systems. In doing so, however, the ERO Enterprise requests that the Commission apply its standards for CEII treatment and protection consistent with the FERC-NERC whitepaper on CIP Violations.[15] The Commission stated in the NOPR that its regulations provide for "any person who is a participant in a proceeding or has filed a motion to intervene or notice of intervention to make a written request to the filer for a copy of the complete, non-public version of the document."[16] The ERO Enterprise urges the Commission to consider how this information would be protected in these public proceedings. Similarly, the ERO Enterprise urges the Commission to carefully consider what information is necessary for the proposed additional reporting requirements.[17]

---

15 FERC and NERC, *Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards*, Docket No. AD19-18-000 (Sep. 2020), https://www.ferc.gov/sites/default/files/2020-09/Second%20Joint%20White%20Paper_CIP%20NOP%20Confidentiality_09.23.2020_AD19_18_000_0.pdf.

16 NOPR at P 74.

17 *Id.* at P 64.

The ERO Enterprise also seeks clarification on whether it needs to intervene in every proceeding to obtain protected or CEII information, or whether there will be a separate process for communication between the utilities and relevant regulatory authorities. The ERO Enterprise is concerned that the proposed protective order for third parties may prohibit the ERO Enterprise's ability to be a valid intervenor under the Commission's regulations, and thus be unable to access critical and necessary information as part of the application and verification process for cybersecurity incentives.

Finally, from a technical standpoint, the ERO Enterprise urges the Commission to consider whether the proposed hub-spoke approach may introduce additional attack vectors to medium and high impact BES Cyber Systems through increased connectivity.

C. The Commission should consider implications for the NERC standards development process.

The ERO Enterprise has the authority to develop Reliability Standards pursuant to its statutory and regulatory duties.[18] This process is outlined in the *Standard Processes Manual*, Appendix 3A to the NERC Rules of Procedure.[19] As part of this process, industry stakeholders vote on requirements that help to maintain reliability of the Bulk-Power System. This voting results in a consensus product that represents controls to support reliability based on industry expertise.

While the ERO Enterprise appreciates the Commission's efforts to encourage industry to adopt stronger practices voluntarily, the ERO Enterprise is concerned that it may create financial reasons to oppose the standards development process. As noted above, industry stakeholders have a significant role in the standards development process. If their companies may lose an advantage with a standard becoming mandatory, these voluntary incentives may provide a reason for

[18] 16 U.S.C. § 824(o)(e) (2018); 18 C.F.R. § 39 (2020).

[19] The NERC Standard Processes Manual is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

individuals to stop participating in the process or even obstruct the standards development process, which could slow down development. As a result, the ERO Enterprise requests the Commission: (1) consider a process for removing incentives as certain practices transition from voluntary to mandatory; and (2) consider the implications for industry's involvement in the standards development process if it means losing some favorable rate treatment.

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. Nonetheless, the ERO Enterprise urges the Commission to consider implications for its CMEP processes, standards development processes, and other ERO Enterprise activities prior to finalizing the proposed approach. As such, the ERO Enterprise respectfully requests the Commission consider the issues raised in these comments.

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

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
Joshua Yang
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net
joshua.yang@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
lisa.zell@mro.net
Counsel for Midwest Reliability Organization

/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/ Steven F. Goodwill
Steven F. Goodwill
Senior Vice President of Reliability and Security Oversight, General Counsel and Secretary
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6879
sgoodwill@wecc.org
Counsel for the Western Electricity Coordinating Council

/s/ Kristin McKeown
Kristin McKeown
General Counsel and Secretary
Northeast Power Coordinating Council, Inc.
1040 Ave. of the Americas, 10th Floor
New York, NY 10018
(212) 840-1070
kmckeown@npcc.org
Counsel for Northeast Power Coordinating Council, Inc.

Date: April 6, 2021