UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE PUBLIC UTILITIES COMMISSION OF OHIO'S OFFICE OF THE FEDERAL ENERGY ADVOCATE

To implement Section 40123 of the Infrastructure Investment and Jobs Act of 2021 ("IIJA"), the Federal Energy Regulatory Commission ("FERC" or the "Commission") issued a Notice of Proposed Rulemaking ("NOPR") in September 2022 to create incentives for voluntary cybersecurity measures to protect the bulk power system's ("BPS") operations. Incentive-based rate treatments would be made available to utilities that invest in cybersecurity to "enhance their security posture by improving their ability to protect against, detect, respond to, or recover from a cybersecurity threat and to utilities that participate in cybersecurity threat information sharing programs to the benefit of ratepayers and national security."[1] Given ongoing grid modernization, the expansion of telework since the outbreak of COVID-19, and rising concerns about the vulnerability of the grid, the Commission is right to take up concerns about cybersecurity. The Public Utilities Commission of Ohio's Office of the Federal Energy Advocate ("Ohio FEA") appreciates the importance of this matter but cautions that the proposed

[1] NOPR at ¶ 1.

incentives for voluntary cybersecurity investments may lead to unjust and unreasonable rates for ratepayers.

I. BACKGROUND

In 2006, FERC implemented an amendment to the Federal Power Act ("FPA") to require reliability standards, including cybersecurity protection, and designated the North American Electric Reliability Corporation ("NERC") to enforce the standards. Since their adoption in 2008, NERC's Critical Infrastructure Protection ("CIP") Reliability Standards have been modified to the current 13 standards to ensure the cyber and physical security of the BPS. Of them, 12 cybersecurity standards are currently effective.[2]

In 2019, the Commission issued a Notice of Inquiry seeking comment on the scope and implementation of its electric transmission incentives policy to ensure that the policy continues to satisfy its obligations under FPA Section 219.[3] In 2020, the Commission issued a Notice of Proposed Rulemaking on transmission incentives and stated that cybersecurity would be addressed in a separate proceeding. In June 2020, Commission staff issued a white paper suggesting a framework for incentives under FPA Section 219 to "allow the electric industry to be more agile in monitoring and responding to new and evolving cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions."[4] In December 2020, the Commission issued a Notice of Proposed Rulemaking on

---

[2] United States Mandatory Standards Subject to Enforcement, available at https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.

[3] *Inquiry Regarding the Commission's Electric Transmission Incentives Policy*, 166 FERC ¶ 61,208 (Mar. 21, 2019).

[4] *Cybersecurity Incentives*, Docket No. RM21-3-000, Notice of Proposed Rulemaking (Dec. 17, 2020), at 15.

cybersecurity incentives in Docket No. RM21-3, and accepted comments on its proposal. In November 2021, Congress passed the IIJA, which calls, in part, for more than $50 billion to be invested to improve infrastructure resilience to climate change, cybersecurity attacks, and extreme weather events. The IIJA directs FERC to establish incentive-based rate treatments for certain voluntary cybersecurity investments. FERC responded with a new cybersecurity NOPR and terminated the prior proceeding.

The current NOPR would provide incentive-based rates for transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce to encourage: (1) investments by utilities in advanced cybersecurity technology; and (2) participation by utilities in cybersecurity threat information sharing programs. The IIJA calls for a final rule by May 2023.[5]

Incentive-eligible cybersecurity expenditures would be required to: (1) materially improve cybersecurity through either an investment in advanced cybersecurity technology or participation in cybersecurity threat information sharing programs; and (2) not be mandated by CIP Reliability Standards or local, state, or federal law. The draft NOPR proposes a list of pre-qualified investments ("PQ List") to identify the types of cybersecurity expenditures that the Commission may find eligible for incentives. The NOPR also seeks comment on a case-by-case approach to incentive requests. The Commission proposes two incentives: (1) a return on equity ("ROE") adder of 200 basis points for eligible cybersecurity investments; and (2) deferred cost recovery for certain

[5] 16 U.S.C. § 824s-1(c).

cybersecurity-related expenditures and inclusion of the unamortized portion in rate base. Certain incentives would be subject to a five-year sunset provision.

The Ohio FEA continues to support efforts to protect the BPS from cybersecurity attacks on the grid. But as we stated in reply comments in the earlier cybersecurity proceeding and pointed out above, FERC appointed NERC to establish cybersecurity standards and NERC has responded with 12 of them. To enable utilities to envision their own versions of additional measures – at a cost to ratepayers – opens the door to potentially unnecessary investments. While the Ohio FEA recognizes that Congress has required the creation of rules for incentive-based rates for cybersecurity investments, we urge caution to ensure those incentives are just and reasonable.

II. COMMENTS

Given fast-paced grid modernization efforts, unprecedented global events, and rising concerns about the vulnerability of the grid, the Commission is right in its attempt to support investments in advanced cybersecurity technology and to implement Congress's directives on incentives for cybersecurity investments, as mandated by the IIJA. The IIJA amends Part II of the FPA by requiring incentives for certain cybersecurity investments and directs the Commission to establish incentive-based rate treatments for the transmission and sale of electricity to encourage investment in advanced cybersecurity technology and information sharing by public utilities.[6] FERC

[6] 16 U.S.C. § 824s-1. "Advanced cybersecurity technology" is defined as any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances the security posture of public utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat. 16 U.S.C. § 824s-1(a)(1).

also proposes to include non-public utilities in incentive eligibility.[7] This extension of eligibility would include many smaller entities, such as cooperatives and municipalities, that may be eligible for a whole range of other IIJA cybersecurity incentives.[8]

The Ohio FEA appreciates the Commission's immediate attention to Congress's directives, but remains cautious about incentives for cybersecurity investments,[9] in that they could be arbitrary and complimentary "FERC candy"[10] for utilities that will result in unjust and unreasonable rates for ratepayers.

A. Proposed Approaches to Request an Incentive

The Commission proposes that the utility seeking an incentive must demonstrate, at a minimum, that the expenditure would materially improve cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program and that the expenditure is not already mandated by CIP Reliability Standards, or by local, state, or federal law.[11]

The Ohio FEA believes that eligibility criteria must be in place to limit what could possibly be a large pool of applicants seeking cybersecurity incentives, but respectfully notes the ambiguity in the terms "at a minimum" and "materially improve." Until FERC

---

[7] As FERC notes, the IIJA requires that incentives be offered only to "public utilities." The NOPR also proposes to make rate incentives available to non-public utilities that have or will have a rate on file with FERC, consistent with Commission precedent under FPA Section 219. NOPR at ¶ 1 n.3.

[8] The IIJA includes funding for new and existing cybersecurity-specific programs that focus on strengthening cyber systems and defense against future attacks. *See* https://www.nga.org/news/commentary/opportunities-for-cybersecurity-investment-in-the-bipartisan-infrastructure-investment-and-jobs-act/ and https://www.ncsl.org/ncsl-in-dc/publications-and-resources/infrastructure-investment-and-jobs-act.aspx?adlt=strict.

[9] Ohio FEA Reply Comments in Docket RM21-3-000, at 1.

[10] *See* Remarks of Commissioner Mark Christie, Commission Meeting Transcript September 22, 2022 at 39-40.

[11] NOPR at ¶ 20.

expounds these parameters in detail, they will provide wide latitude for interpretation and fail to achieve the objective of streamlining the review of advanced cybersecurity incentive filings. FERC proposes to reference several federal government cybersecurity resources in determining whether an expenditure would materially improve cybersecurity, including the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, NIST SP 800-53, guidance from the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency or the Department of Energy ("DOE"), and others.[12] While the Ohio FEA agrees that the Commission stands to benefit from the expertise of other federal agencies, the final determination of whether a cybersecurity expenditure will significantly improve a utility's security posture will have to be based on each individual utility's cyberattack experience, mitigation strategy, and, ultimately, its own best interests. Accordingly, the Ohio FEA finds that the eligibility criteria proposed by the Commission may cover too broad a range of utility cybersecurity efforts and should, therefore, be more clearly defined in the final rule.

Regarding investments in advanced cybersecurity technology, the Commission particularly seeks guidance on whether and how it should evaluate the cost-benefit ratio of the cybersecurity expenditure and incentive, in order to ensure that proposed rates are just and reasonable. Admittedly, the impact of cybersecurity investment is more complicated than other utility measures, especially given that the occurrence of an event is largely out of the control of FERC and the utility. The Ohio FEA suggests the use of

[12] NOPR at ¶ 21.

scenarios as described in NARUC's Guidelines for Energy Regulators.[13] Under this approach, the economic items that compose the evaluation have to be calculated in four possible scenarios derived from combinations of two dimensions: the presence/absence of cybersecurity measures, and the presence/absence of a relevant attack. Such scenarios would capture both the proactive and reactive aspects of advanced cybersecurity measures/countermeasures.

With respect to participation in a cybersecurity threat information sharing program, the Ohio FEA can understand hesitation and the lack of transparency on the part of utilities, especially when it comes to critical energy/electric infrastructure information with utility-specific engineering, vulnerability, and detailed design information about proposed or existing critical infrastructure. However, in the face of increasing risks of cyberterrorism, utilities need to be aware of the resources available to help them combat this serious threat. The National Cyber Security Division ("NCSD") of the DHS, with its primary responsibility within the federal government for combating cyberterrorism, administers the Protected Critical Infrastructure Information Program to encourage private industry to share confidential information on the nation's critical infrastructure with the assurance of protection from public disclosure. The Ohio FEA believes that participation in NCSD's cyber-response programs, which include cyberthreat information sharing such as the National Cyber Alert System, US-CERT, National Cyber Response Coordination Group, and the Cyber Cop Portal, should satisfy the eligibility criteria and

[13] Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators ("NARUC Guidelines"), at 23-24, available at https://www.naruc.org/international/news/evaluating-the-prudency-of-cybersecurity-investments-guidelines-for-energy-regulators/?adlt=strict.

would lend not only to the cause of utility cybersecurity but also to national cybersecurity.

B. Proposed Approaches for Evaluating Cybersecurity Expenditure Eligibility

The Commission proposes to use a PQ List or, alternatively, a case-by-case approach to identify the cybersecurity expenditures that the Commission will find eligible for an incentive.[14] Initially, the PQ List would include two eligible cybersecurity expenditures: (1) expenditures associated with participation in the DOE Cybersecurity Risk Information Sharing Program; and (2) expenditures associated with internal network security monitoring within the utility's cyber systems.[15] Expenditures that are included in the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive.[16] Under FERC's proposed alternative approach, advanced cybersecurity incentives would be evaluated on a case-by-case basis with the burden on the utility to prove that the expenditure would result in material improvement and that there is no overlap with local, state, or federal requirements.[17] There would be no presumption of eligibility for any given cybersecurity expenditure. FERC also notes that, under either approach, the utility would be required to demonstrate that its proposed rate, inclusive of the incentive, is just and reasonable.[18]

---

14 NOPR at ¶ 23.
15 NOPR at ¶ 28.
16 NOPR at ¶ 26.
17 NOPR at ¶ 32.
18 NOPR at ¶ 32.

The Ohio FEA believes that a PQ List of investments may be inadequate and incomplete in the vast and ever-changing landscape of cybersecurity. There will never be a definitive list of strategic measures or countermeasures to make the power system more secure. Furthermore, because investments to address cybersecurity often fall into other categories and are seldom "cyber-specific," it may be hard to differentiate them from other utility investment costs.[19] The Commission itself recognizes that the PQ List would have to be reviewed and updated on a regular basis, which will introduce process delays.[20]

The limited eligibility categories proposed by the Commission may inherently lead to a preference for FERC's alternative case-by-case approach, especially given the numerous cybersecurity programs initiated by the IIJA. The case-by-case treatment of cybersecurity investment review may not achieve the efficacy that the advanced cybersecurity incentives in this NOPR are intended to achieve when compared to the review within the foundational CIP Reliability Standards framework. The Ohio FEA, therefore, believes that the proposed incentive-based treatment and accompanying review process would only serve to fill the gaps in cybersecurity threat mitigation that cannot be avoided due to regulatory lag and the time taken to update or develop new CIP Standards.[21]

---

[19] NARUC Guidelines at 17.

[20] NOPR at ¶ 27.

[21] *See* Remarks of Commissioner Allison Clements, Commission Meeting Transcript September 22, 2022 at 37-38.

C. Proposed Rate Incentives

FERC proposes two types of incentives that a utility could receive for an eligible cybersecurity expenditure: a ROE adder of 200 basis points or deferred cost recovery for certain cybersecurity expenditures that would enable the utility to defer expenses and include the unamortized portion in rate base.[22] The Ohio FEA believes that a ROE incentive will encourage public utilities to proactively make additional investments in their cybersecurity systems. We maintain, however, that a 200-basis-point adder is too high an incentive for encouraging public utilities to improve their systems' cybersecurity above and beyond NERC's requirements.

The Ohio FEA previously noted that a ROE adder of 200 basis points for cybersecurity measures is arbitrary and requested clarity as to how the Commission arrived at this number.[23] In the notice of proposed rulemaking in 2020 regarding transmission incentives, the Commission proposed an additional 50-basis-point ROE adder for transmission projects that provide significant and demonstrable reliability benefits above and beyond NERC reliability standards. The Ohio FEA did not, at that time, support a 50-basis-point ROE incentive for such projects based on a lack of evidence.[24] The law that required this NOPR expressly states that the incentives – and any FERC rule revisions for those incentives – must be just and reasonable.[25] Accordingly, FERC Commissioner Phillips has invited stakeholders to comment on

---

22 NOPR at ¶ 33.
23 Ohio FEA Reply Comments in Docket RM21-3-000, at 11.
24 Ohio FEA Comments in Docket RM20-10-000, at 11.
25 16 U.S.C. § 824s-1(e)(1).

whether a 200-basis-point adder is reasonable.[26] The Ohio FEA believes that it is not, and that individual filings seeking the 200 basis points will likewise be in excess of what is just and reasonable. The Ohio FEA is concerned with the lack of evidence to support an excessive 200-basis-point ROE adder. FERC has not shown that this amount is just and reasonable as an incentive for voluntary cybersecurity measures that would only augment a utility's cybersecurity above compliance with mandatory CIP Reliability Standards.

FERC also seeks comment on whether and how the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.[27] In a performance-based rates context, the indicators to assess cybersecurity performance, the minimum levels for these indicators, and the incentive framework adopted would be of great importance. Under FERC's proposal, the utilities could have the freedom to decide which approaches to adopt, investments to carry out, and procedures and processes to implement,[28] which may be advantageous in that utilities can tailor cybersecurity investment according to their specific cybersecurity needs.

Performance indicators for the cybersecurity measures contemplated in the IIJA are relatively uncharted territory. For FERC to determine what it expects from the utilities in terms of cybersecurity investment, the Commission should determine what

---

[26] Phillips Concurrence at ¶ 7.

[27] NOPR at ¶ 44. With respect to the FPA's requirement that incentive-based, including performance-based, rate treatments be established for certain cybersecurity investments, FERC notes that, consistent with precedent, it interprets this provision to consider performance-based rates as an option among incentive ratemaking treatments. NOPR at ¶ 45 n. 41.

[28] NARUC Guidelines at 11.

outcomes are expected, so that stakeholders can strategize accordingly.[29] It is also important for FERC to determine in advance how it will interact with the utilities, not only on how the utilities brief regulators but also on continuous reviews, which should include incident reporting. This will ensure a more efficient process overall.

If the Commission adopts performance-based rates for cybersecurity incentives, FERC should neither choose which expenses to approve nor check whether incurred expenses comply with the utility's plans, but should simply verify whether predetermined outcomes have been achieved. The Ohio FEA recommends that FERC consider developing resources, such as the DOE's Cybersecurity Capability Maturity Model (C2M2),[30] to achieve a performance monitoring tool that will aid in performance-based rates.

D. Proposed Incentive Implementation

FERC proposes that a utility that has received cybersecurity incentives would be required to submit an annual informational filing detailing the specific investments that were made pursuant to the Commission's approval and the corresponding FERC account for which expenditures are booked.[31] The Ohio FEA believes that more is needed. In this context, the Ohio FEA notes that the IIJA prohibits duplicate recovery for these cybersecurity incentives: "[a]ny rule * * * shall preclude rate treatments that allow unjust

---

[29] Black Sea Cybersecurity Strategy Development Guide, at 10, available at https://pubs.naruc.org/pub/E20048B4-155D-0A36-3117-F2F0A7A692F4?adlt=strict.

[30] Available at https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[31] NOPR at ¶ 55.

and unreasonable double recovery for advanced cybersecurity technology."[32] Therefore, the Ohio FEA recommends that, with the Commission's adoption of advanced cybersecurity incentives, verification methods should be established that go beyond the annual information filings proposed by FERC. This includes safeguards to ensure that cybersecurity benefits are realized and that double recovery of incentives is avoided.

E. Other Recommendations

The Commission should continue to direct NERC to review its CIP Reliability Standards. The Ohio FEA believes that this NOPR should not detract from the necessary, albeit slow, administrative process of updating or expanding mandatory CIP Standards to accommodate current and best practices in cybersecurity measures. In parallel to this NOPR, the Ohio FEA recommends that FERC should continue to work with NERC to update and expand mandatory CIP Standards.

As the BPS is highly interconnected and interdependent, the Ohio FEA reiterates its support for mandatory CIP Standards that require compliance by all responsible entities and thereby increase the overall reliability of the system.

III. CONCLUSION

The Ohio FEA asserts that the importance of attention to cybersecurity cannot be overstated, and the IIJA's attention to the matter is justified. But the NOPR suggests measures that are ambiguous and overly generous. The proposed 200-basis-point reward for potentially unnecessary investment is excessive and may lead to unjust and

[32] 16 U.S.C. § 824s-1(e)(2).

unreasonable rates. FERC's suggested PQ List is unlikely to keep up with evolving threats and case-by-case reviews are subject to regulatory lag and inefficiency. Under FERC's proposal, double recovery of investments and incentives may remain a possibility as well. The Ohio FEA urges the Commission to continue to rely on NERC to address the evolving cybersecurity landscape, leaving it to the reliability overseer to require new measures as they become necessary. If the Commission were to do so, many of the remaining questions on cybersecurity preparedness addressed in this NOPR may resolve themselves.

Respectfully submitted,

Dave A. Yost
Ohio Attorney General

John H. Jones
Section Chief

/s/ Thomas G. Lindgren
Thomas G. Lindgren
Assistant Attorney General
Public Utilities Section
30 East Broad Street, 26th Floor
Columbus, Ohio 43215-3414
614.644.8768 (telephone)
866.818.6152 (facsimile)
Thomas.Lindgren@OhioAGO.gov

On Behalf of the Federal Energy Advocate
The Public Utilities Commission of Ohio

November 7, 2022

CERTIFICATE OF SERVICE

I hereby certify that I have on this date caused a copy of the foregoing document to be served on each person included on the official service list maintained for this proceeding by the Commission's Secretary, by electronic mail or such other means as a party may have requested, in accordance with Rule 2010 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.2010. Dated this the 7th day of November 2022, at Columbus, Ohio.

/s/ Thomas G. Lindgren
Thomas G. Lindgren
Assistant Attorney General