UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

JOINT COMMENTS OF THE MARYLAND PUBLIC SERVICE COMMISSION AND PENNSYLVANIA PUBLIC UTILITY COMMISSION

The Maryland Public Service Commission ("MDPSC") and Pennsylvania Public Utility Commission ("PAPUC") (collectively, "Joint Commissions") submit these comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") on September 22, 2022, in the above-captioned docket. The NOPR proposes incentive-based rate treatments to encourage investments by utilities in advanced cybersecurity technology and participation by utilities in cybersecurity threat information sharing programs, as directed by the *Infrastructure Investment and Jobs Act of 2021* (Infrastructure and Jobs Act or IIJA).[1]

I. COMMUNICATIONS

All pleadings, correspondence, and other communications related to this proceeding should be addressed to the following persons:

Maryland Public Service Commission
6 St. Paul Street
Baltimore, Maryland 21202

Miles H. Mitchell
Deputy General Counsel
Tel: 410-767-2972
miles.mitchell@maryland.gov

[1] 16 U.S.C. § 824s-1 (Incentives for cybersecurity investments).

Ransom E. Ted Davis
Associate General Counsel
Tel: 410-767-8076
ransom.davis@maryland.gov

Morris Schreim
Senior Commission Advisor
Tel: 410-767-3556
morris.schreim@maryland.gov

John Borkoski
Chief Engineer
Tel: 410-767-8069
John.Borkoski@maryland.gov

Trevor Tomlinson, Esq.
Commission Legal Advisor
Tel: 410-767-8017
Trevor.Tomlinson1@maryland.gov

And:

Christopher Van de Verg, Assistant Counsel
Christian McDewell, Assistant Counsel
Elizabeth H. Barnes, Deputy Chief Counsel
P.O. Box 3265
Harrisburg, PA 17105-3265
Telephone: 717-787-5000
Email: cvandeverg@pa.gov
cmcdewell@pa.gov
ebarnes@pa.gov

II. INTRODUCTION

The Joint Commissions agree with FERC about the importance of addressing cybersecurity challenges. However, the Joint Commissions do not agree with FERC's premise that incentives should be necessary to encourage cybersecurity initiatives. Cybersecurity is not new, and implementation of common-sense measures, such as those outlined in the NOPR, constitutes good cybersecurity practice. Public utilities serving the bulk power system should already be implementing those measures. Striving to optimize utilities' cybersecurity posture to

secure the reliability of assets serving electricity customers at the lowest cost to ratepayers should likewise already be ingrained within a public utility's corporate culture. Accepting that the Commission has a statutory mandate to issue new rules providing for cybersecurity incentives, and for the Commission's consideration in issuing a final rule, the Joint Commissions offer the following comments and observations, emphasizing upfront that incentives should be limited and targeted.

III. COMMENTS

FERC proposes that qualification for cybersecurity expenditure incentives be evaluated against two eligibility criteria: (1) that the expenditure materially improves cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program; and (2) that the expenditure is not already mandated by CIP Reliability Standards or local, state, or Federal law.[2] FERC identifies a lengthy list of sources for eligible expenditures, including security controls enumerated in National Institute of Standards and Technology (NIST) 800-53, security controls satisfying an objective in the NIST Cybersecurity Framework, specific recommendations by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA), or the Department of Energy (DOE), and similar sources.[3]

FERC further proposes adopting a pre-qualified list (PQ List) approach, whereby FERC would create a list of expenditures that could warrant an incentive, and a utility seeking an incentive would be required to demonstrate that its cybersecurity expenditure qualifies as one or more of the PQ List items.[4] Any cybersecurity expenditure that is on the PQ List would be

[2] NOPR, ¶ 20.
[3] NOPR, ¶ 21.
[4] NOPR, ¶¶ 25-26.

entitled to a rebuttable presumption of eligibility for an incentive, although utilities would still need to demonstrate, and the Commission would need to find, that the proposed rate, inclusive of the incentive, is just and reasonable. [5] Intervening parties could rebut this presumption by demonstrating that the cybersecurity expenditure does not meet one or more of the eligibility criteria, or the Commission could make this finding *sua sponte*.[6] The NOPR states that the PQ List approach will provide a transparent and efficient mechanism for evaluation of cybersecurity expenditures.[7]

As an alternative to the PQ List approach, FERC describes (but does not propose) a "case-by-case approach," whereby a utility would apply to receive incentives for cybersecurity expenditures, based on a showing that the expenditures satisfy FERC's proposed eligibility criteria. There would be no rebuttable presumption, and the utility would have the burden to demonstrate that the expenditures meet the eligibility criteria and that its proposed rate is just and reasonable.[8] However, the case-by-case approach may challenge FERC's internal staffing resources in terms of time and expertise.

A. The Pre-Qualified List Approach

Joint Commissions acknowledge the benefits of streamlining the incentives process through the selection and use of pre-qualified cybersecurity measures, given the commonality in cybersecurity challenges some utilities face. The PQ List approach has the potential to upgrade utilities' cybersecurity posture while conserving FERC's internal resources as compared to the case-by-case approach.

[5] NOPR, ¶ 26.
[6] NOPR, ¶ 26.
[7] NOPR, ¶ 3.
[8] NOPR, ¶ 32.

However, while cybersecurity threats grow and associated expenditures evolve, FERC's proposal to update the PQ List raises concerns. FERC states that it expects to regularly evaluate the PQ List and update it as necessary via a rulemaking based on the existing or modified eligibility criteria.[9] Further, if a cybersecurity expenditure on the PQ List becomes mandatory, it would no longer be eligible for the incentive as of the effective date of the mandate.[10] Given the potentially lengthy process involved in updating a list through rulemaking, the PQ List approach might challenge FERC's ability to update the List in real-time to match the current threat environment. If FERC cannot keep the PQ List current, there could be (1) overinvestment in outdated measures, simply because they remain on the List, and (2) underinvestment in cutting-edge measures, simply because they are not on the List, thereby diminishing competition and innovation in the cybersecurity marketplace.

While regular updates of the PQ List might enable FERC to respond to emerging cybersecurity needs, revisions to the list will create new timing challenges for both FERC and applicants with respect to which cybersecurity investments are incentivized and when they are incentivized. These timing challenges will be heightened in that (1) the FERC rulemaking process to update the List is lengthy and unpredictable, by which time any proposed new expenditure may become obsolete; and (2) cybersecurity expenditures may take utilities years to budget, plan and deploy, by which time the expenditure may no longer be on the List.

Joint Commissions have serious reservations about allowing utilities to rely on a rebuttable presumption, which appears to be the key feature of the PQ List approach. The presumption unfairly places the burden on ratepayers and their advocates to discern the details of the utility applicant's implementation and determine whether that implementation was conducted

[9] NOPR, ¶ 31.
[10] NOPR, ¶ 31.

in a just and reasonable manner. Utilities have easy access to this information but ratepayers have little or none. This burden will be exacerbated in that much of the sought-after information will likely be designated as critical energy/electric infrastructure information (CEII).[11] Moreover, this rebuttable presumption is wholly inconsistent with the FERC's incentive structure for transmission projects under Section 219 of the Federal Power Act.[12]

Joint Commissions further caution that FERC's proposed PQ List approach could drive utilities to invest in the listed measures to the exclusion of other measures regardless of their relative merits. Utilities could be tempted to deploy a listed technology, not on the basis of particularized cybersecurity need, but primarily for the sake of obtaining the incentive. Such an investment could, in turn, cause the utility to prematurely declare a prior technology investment to be obsolete, resulting in an unusable, stranded asset.

In a related vein, Joint Commissions are also concerned that FERC's proposed incentives could encourage utilities to direct cybersecurity expenditures towards PQ items instead of other, more effective cybersecurity expenditures that are not on the PQ List. Joint Commissions expect that utilities make cybersecurity expenditures at the holding company level. That is, many transmission owner (TO) utilities are owned by a parent holding company, which in turn also owns one or more state-specific electric distribution companies (EDCs). Functions such as cybersecurity are often implemented on an enterprise-wide basis through a common platform.

When the holding company makes a cybersecurity expenditure (including one to which FERC's proposed incentives apply), the costs flow down to the holding company's TO and EDC subsidiaries, according to the holding company's intra-company agreements. However, it is possible that an expenditure associated with FERC's incentive proposal may not provide

[11] 18 CFR § 388.113.
[12] 16 U.S.C. § 824s.

appreciable benefits to the EDC. A state EDC's customers may thus be saddled with the costs of a PQ List item when a different cybersecurity expenditure may better suit the EDC and its customers.

In sum, while the items on the PQ List may have merit in the abstract, the proposed incentives have the potential to influence the cybersecurity needs of state-regulated EDC affiliates of TOs towards the measures on the PQ List, regardless of their applicability or benefit to the EDC and its customers. While such "trickle down" effects are perhaps unavoidable, their existence only increases the importance that the PQ List includes cybersecurity measures that truly provide benefit to ratepayers through increased reliability.

B. The Case-by-Case Approach

Joint Commissions see merit in aspects of the case-by-case approach to determining utility eligibility for incentives. Compared to the PQ List approach, the case-by-case approach is better tailored to the individualized needs and circumstances of utilities.[13] This approach would allow utilities to demonstrate their case for incentives based on actual need or adherence to the statutory criteria that are specific to the utility. In addition, a case-by-case approach allows utilities to be more innovative in their cybersecurity improvements, whereas a PQ List incents utilities to invest in standards which may always be slightly behind the curve. Finally, the case-by-case approach would facilitate the examination of the applicant's deployment of expenditures holistically, throughout a holding company's TO and EDC affiliates. This could alleviate the problems associated with the "trickle down" effects Joint Commission identify, above.

[13] *See*, Initial Comments of the Edison Electric Institute, FERC Docket No. RM21-3-000, *Cybersecurity Incentives* (Apr. 6, 2021) ("Properly crafted, incentives can help utilities to prioritize investments that will enhance the cybersecurity of their assets. Accordingly, recognizing the voluntary and often utility specific decisions to make investments that benefit customers by seeking incentives, EEI urges the Commission not to presume that all investments are appropriate for all utilities.").

While the case-by-case approach gives utilities the initiative to identify their individual cybersecurity priorities, this is not to say that FERC will have no role in guiding good investment. FERC's oversight of NERC and the adoption of CIP Reliability Standards could play a predominant role in guiding policy. By using the case-by-case approach, public utilities may inform NERC and FERC of innovative solutions which could become standard industry-wide. So too, FERC's ratemaking process will create the opportunity to review expenditures and FERC may exercise further guidance and discretion through that mechanism.

C. State Law Requirements

FERC proposes that a utility is not eligible for incentives to the extent that the proposed cybersecurity expenditure is already mandated by the CIP Reliability Standards, or local, state, or Federal law.

Joint Commissions believe that the list of requirements for which incentives are not eligible should be clarified. FERC states that utilities would not be eligible for incentives if the cybersecurity expenses on the subject practice were "mandated by local, state, or Federal law."[14] FERC should clarify that "local, state, or Federal law" includes all elements of compliance, such as federal agency requirements like Federal Trade Commission (FTC) decisions, state commission regulations and orders, court orders, and state attorneys general directives that address cyber security requirements or expectations of good cybersecurity practice. This will ensure that utilities do not receive incentives for implementing measures which they should be implementing already.

Even if these requirements/mandates are specific only to electric distribution, EDCs are often affiliates of transmission companies and their cyber security programs are expected to be

[14] NOPR, ¶46.

managed under a single corporate umbrella. What is applied at the distribution level may be implemented corporate-wide. Therefore, FERC should clarify whether a utility is eligible for incentives for an expenditure if an affiliated company has a legal requirement to make that expenditure. To receive the incentive, the utility should bear the burden of demonstrating that its program is distinct and separate from its affiliate and receives no common corporate oversight or direction as to cybersecurity.

In suggesting incentives for the PQ List, the NOPR neglects to recognize that some utilities are members of Regional Transmission Organizations (RTOs) that already participate in information sharing programs, specifically the Cybersecurity Risk Information Sharing Program (CRISP), a program that has been in existence for almost a decade. For instance, PJM testified to the Senate Energy and Resources Committee that:

> Our government partners do a great job of sharing threat information as appropriate. We rely on our government partners to share relevant information that we can use to protect our systems. The Electricity Information Sharing and Analysis Center (E-ISAC) is the hub of information sharing for the electric industry and continues to evolve its information-sharing programs. In addition, we receive threat indicators from the Department of Homeland Security and government-informed analysis from the Cyber Risk Information Sharing Program (CRISP).[15]

To represent this level of involvement to the Committee, PJM necessarily interfaces with the electric utilities whose assets it is charged with operating and planning. As such, utility members of PJM already satisfy the CRISP communications initiative in FERC's proposed PQ List.

D. Incentive and Timeline

[15] Testimony of Thomas O'Brien, Senior Vice President and Chief Information Office, PJM Interconnection, L.L.C. before the U.S. Senate Energy and Natural Resources Committee (Aug. 5, 2020), available online at: https://www.energy.senate.gov/services/files/C21F67A4-547A-4A8F-9036-8DAB9EF02DE2

Joint Commissions believe that FERC's proposed incentives do not (1) encourage the earliest possible adoption and deployment of technologies and programs that will materially improve utility cybersecurity; nor (2) avoid a perverse incentive whereby the availability of incentives for certain items delays adoption of those same items as CIP Reliability Standards or other requirements.

As Commissioner Phillips' concurrence recognizes, ¶ 1, CIP Reliability Standards are baseline requirements that can take years to implement. The NOPR suggests that incentives will result in material improvements to utility cybersecurity, even while new CIP standards developed and eventually enacted. But the NOPR does not specifically tie implementation of the desired improvements to the standards development process. Simply making incentives available in the period prior to completion of mandatory standards does nothing to expedite the standards process or the adoption of voluntary improvements. In fact, FERC's proposals suggest that it is acceptable for standard development to lag because utilities can be incented to voluntarily implement improvements. The Joint Commissions note that the NOPR neglects to explore having incentives taper off over a prescribed time frame (e.g., over the average time frame in which a CIP standard is developed), in anticipation of CIP standards being completed. Such a provision could drive utilities to implement material improvements as early as possible. It would also add a "performance-based" aspect to FERC's proposals, consistent with the IIJA.

E. The Proposed Initial PQ List

FERC proposes just two eligible cybersecurity expenditures for the initial PQ list: (1) expenditures associated with participation in CRISP and (2) expenditures associated with internal network security monitoring within the utility's cyber systems.[16] FERC provides little or

[16] NOPR, ¶28.

no explanation why these two expenditures were selected over the myriad of other expenditures relating cybersecurity for utilities.[17]

Also, the IIJA defines "advanced cybersecurity technology" to encompass "any technology… 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."[18] Compared to that broad statutory definition, the proposed initial PQ List focuses on two specific expenditures. While the NOPR seeks comment on "other cybersecurity expenditures", it is concerning that FERC proposes these two expenditures with little explanation as to how they were deemed to provide meaningful improvements to cybersecurity posture.

F. Alternatives

While FERC proposes two positive incentives – an ROE adder and deferred cost recovery – FERC does not address the potential for application of other possible incentive-based rates which are permissible under the statutory requirement. The IIJA requires that FERC implement "incentive-based, including performance-based, rate treatments."[19] The Joint Commissions would note that an "incentive-based" rate treatment includes not only ROE adders to provide additional revenue in support of new cybersecurity programs, but may also include penalties for continuing to use antiquated cybersecurity measures. Performance-based rates are likewise included under the IIJA's mandate. The Joint Commissions encourage FERC to explore performance-based mechanisms as a viable means of securing material improvements in utilities' cybersecurity posture.

[17] NOPR, ¶¶ 14-15.
[18] 16 U.S.C. § 824s-1(a)(1).
[19] 16 U.S.C. § 824s-1(a)(1).

IV. CONCLUSION

The Joint Commissions respectfully request the Commission to consider these comments.

Respectfully submitted,

H. Robert Erwin, Jr.
General Counsel

s/ ***Miles H. Mitchell***
Miles H. Mitchell
Deputy General Counsel
Tel. 410-767-2972
miles.mitchell@maryland.gov

Ransom E. Ted Davis
Tel. 410-767-8076
ransom.davis@maryland.gov

/s/ Christopher F. Van de Verg
Christopher F. Van de Verg, Assistant Counsel
Christian A. McDewell, Assistant Counsel
Elizabeth H. Barnes, Deputy Chief Counsel
Renardo L. Hicks, Chief Counsel
Pennsylvania Public Utility Commission
P.O. Box 3265
Harrisburg, PA 17105-3265
Telephone: 717-787-5000
cvandeverg@pa.gov
cmcdewell@pa.gov
ebarnes@pa.gov
rehicks@pa.gov
Counsel for the Pennsylvania
Public Utility Commission

Dated: November 7, 2022

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that I am on this date serving a copy of the foregoing comments upon each person designated on the official service list compiled by the Federal Energy Regulatory Commission in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure.

Respectfully submitted,

/s/ Christopher F. Van de Verg
Christopher F. Van de Verg
Assistant Counsel
Counsel for the Pennsylvania Public Utility Commission

P.O. Box 3265
Harrisburg, PA 17105-3265
Tel: (717) 787-5000

Dated: November 7, 2022