UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

INCENTIVES FOR ADVANCED CYBERSECURITY INVESTMENT	**DOCKET NOS. RM22-19-000**
CYBERSECURITY INCENTIVES	**RM21-3-000**

COMMENTS OF THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

The National Rural Electric Cooperative Association ("NRECA") respectfully submits comments in response to the Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives Notice of Proposed Rulemaking published by the Federal Energy Regulatory Commission ("Commission") in the above-captioned dockets on September 22, 2022.[1] In the NOPR, the Commission proposes revisions to its regulations to provide incentive-based rate treatments for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities for the purpose of benefitting consumers by encouraging 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").

NRECA appreciates the opportunity to submit comments in response to the NOPR and requests that the Commission exercise caution if it elects to move forward in implementing incentives to encourage cybersecurity investments that exceed the requirements of the North

[1] *Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives*, Notice of Proposed Rulemaking, Docket Nos. RM22-19-000, *et al.* (issued September 22, 2022) ("NOPR").

American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards for the reasons described below.

I. DESCRIPTION OF NRECA

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power one in eight Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landmass.[2]

Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 63 generation and transmission ("G&T") cooperatives and 831 distribution cooperatives. The G&T cooperatives generate and transmit power to distribution cooperatives that provide it to the end of line co-op consumer-members. Collectively, G&T cooperatives generate and transmit power to nearly 80 percent of the distribution cooperatives in the nation. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

NRECA's member cooperatives include Registered Entities subject to the Reliability Standards developed by NERC and approved by the Commission pursuant to section 215 of the Federal Power Act.[3] Nearly all cooperatives, even if they are not Registered Entities, depend on

---

[2] See https://www.electric.coop/electric-cooperative-fact-sheet/.

[3] 16 U.S.C. § 824o (2018).

the Bulk Electric System ("BES") and thus have an interest in the reliability of the BES. Thus, NRECA's member cooperatives have significant interests in the topics of this inquiry.

II. COMMUNICATIONS

Please direct communications concerning this pleading to the following persons and place their names on the Commission's official service list.

Mary Ann Ralls
Senior Regulatory Counsel
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5837
Email: MaryAnn.Ralls@nreca.coop

Jesse Halpern
Thompson Coburn LLP
1909 K Street, N.W.
Suite 600
Washington, DC 20006
Telephone: (202) 585-6900
Email: jhalpern@thompsoncoburn.com

III. COMMENTS

NRECA appreciates the Commission's need to revise its regulations in accordance with the Infrastructure and Jobs Act to establish incentive-based rate treatments that encourage "investments by public utilities in advanced cybersecurity technology and participation by public utilities in cybersecurity threat information sharing programs."[4] However, after reviewing the framework outlined in the NOPR, NRECA requests that the Commission exercise caution as it establishes rules for incentive-based, including performance-based, rate treatments for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities.[5] Under the NOPR, the Commission proposes to add a new

---

[4] NOPR at P 7.

[5] NRECA appreciates the Commission's proposal "to make rate incentives available to non-public utilities that have or will have a rate on file with the Commission, similar to Commission precedent under FPA section 219, 16 U.S.C. 824s" notwithstanding that the Infrastructure and Jobs Act only requires the Commission to offer such incentives to "public utilities." NOPR at n.3.

section 35.48 to the Commission's regulations that "would make incentives available to utilities that make certain cybersecurity expenditures that 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."[6] In the NOPR, the Commission addresses eligibility requirements, incentive types, incentive duration, and reporting requirements. Many of the issues associated with an incentive-based approach to cybersecurity investments addressed in NRECA's comments in Docket Nos. AD20-19 and RM21-3 persist and the Commission's proposed approach raises concerns that the Commission should address before issuing a final rulemaking.

A. PROPOSED ELIGIBILITY CRITERIA AND APPROACHES FOR EVALUATING CYBERSECURITY INCENTIVES

1. The Commission should further define the eligibility criteria for cybersecurity expenditures.

NRECA requests that the Commission consider further defining the eligibility criteria that the Commission proposes to add to its regulations as 18 C.F.R. § 35.48(c). NRECA agrees with the Commission's proposal that, to be eligible, "cybersecurity expenditures must: (1) materially improve cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program; and (2) not already be mandated by Critical Infrastructure Protection (CIP) Reliability Standards, or local, state, or Federal law."[7] However, NRECA is concerned that the phrase "materially improve cybersecurity," even as qualified by the Commission's proposal to consider six sources from agencies responsible

6 NOPR at P 1.

7 *Id.* at P 2.

for addressing cyber threats,[8] remains too subjective to ensure the proposed cybersecurity expenditure provides adequate benefits to ratepayers.

Accordingly, in keeping with its question as to whether it "should evaluate and ensure that the benefits of the expenditure exceed the combined costs of the expenditure and incentive, to ensure the proposed rates are just and reasonable,"[9] the Commission should specify criteria or otherwise establish a minimum level of benefit or value that projects must provide to overall grid security or reliability. Absent such criteria or specifications, the proposed framework may result in utilities "gold-plating" the system on a project-by-project basis rather than focusing on more strategic, reliability-focused projects that would result in broader, measurable improvements to reliability and security. The Commission also should consider specifying whether it will grant incentive-based rate treatment for cybersecurity expenditures that enhance the reliability and security of low impact BES Cyber Systems, or whether it will only do so only for cybersecurity expenditures that enhance the reliability and security of high or medium BES Cyber Systems. Further, by establishing a uniform set of criteria or specifications, the Commission and the industry would be better positioned to review the nation's BES assets using the criteria to determine the overall necessity and urgency of cybersecurity-related investment, necessary changes to the CIP Reliability Standards, or best practices that should be become part of the normal regional planning processes.

In developing the criteria, the Commission should consider specifying the range of enhancements that the Commission would consider acceptable. For example, building

---

[8] *Id.* at P 21.

[9] *Id.* at P 20.

management and fire control systems are automated and continuous monitoring security controls, but seem too far afield from true reliability impacts to be worthy of incentive rate treatment. Including guidance as to what types of enhancements would be considered would help ensure that proposed projects will achieve the intended benefits and reduce the number and scope of applications that interested parties and the Commission will be required to review.

Similarly, the Commission also should consider specifying to which, if any, ongoing costs associated with a cybersecurity investment the incentive-based rate treatment will apply. Under the NOPR, the Commission has defined cybersecurity investments as "expenditures that can be either capitalized costs or expenses."[10] As a result, it is unclear whether an entity that upgrades a low impact substation to incorporate BES Cyber System security controls would receive incentive-based rate treatment for the cost of the upgrade only or also the ongoing costs of operating and maintaining the enhanced security controls. Further, because not all ongoing costs are the same, the Commission should consider whether certain ongoing expenditures should be eligible for incentive-based rate treatment while others should not. Specifications of this nature are especially important where the incentive return on equity ("ROE") adder flows through a formula rate to ensure that the Commission can track the overall cost/rate impacts and determine whether those rate impacts are just and reasonable.

Finally, NRECA requests that the Commission consider whether it is appropriate to confine expenditures that are eligible for incentive-based rate treatment to advanced cybersecurity

[10] *Id.* at n.3.

technology or participation in a cybersecurity threat information sharing program.[11] This proposed approach may limit the ways in which utilities will apply their finite resources. Rather than evaluating a variety of tactics to enhance the security of their BES Cyber Systems, the proposed approach encourages utilities to make investments in technology (for which they can receive incentive-based rate treatment) and not to address their greatest risks. In some cases, a more efficient means of enhancing the security of BES Cyber Systems might be hiring additional staff or contracting with a third-party service provider with specialized expertise and experience. As a result, because the proposed approach incents investment in advanced cybersecurity technology and not the hiring of personnel, utilities may not make the most efficient use of their resources, diminishing the impact of those resources on security of the BES.

2. The Commission should revise its proposed approach to evaluating the eligibility of cybersecurity expenditures for incentive treatment.

NRECA requests that the Commission exercise caution with respect to its proposed "PQ List" approach to evaluating the eligibility of cybersecurity expenditures for incentive-based rate treatment. According to the NOPR, the PQ List would be "a list of pre-qualified expenditures that are eligible for incentives determined by the Commission and publicly maintained on the Commission's website."[12] The PQ List also would "be codified at 35.48(d) of the Commission's regulations."[13] NRECA requests that, before implementing this approach, the Commission consider the potential vulnerabilities that the Commission could create by publishing the PQ List,

---

[11] While Section III.A.1 of the NOPR clearly limits eligibility to "investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program(s)," NOPR at P 20, Section III.B.2 appears to contemplate the deferral of the cost of "training to implement new cybersecurity practices and systems." *Id.* at P 40. NRECA asks that the Commission resolve this inconsistency in any final rule.

[12] NOPR at P 3.

[13] *Id.* at P 25.

particularly a more comprehensive version than that currently envisioned under the NOPR. If the Commission develops and publicly maintains on the Commission's website a comprehensive list of cybersecurity expenditures that are eligible for incentive-based rate treatment, a bad actor may review that PQ List and search eLibrary to identify those utilities that have adopted these measures. That bad actor then will be in a position to tailor attacks on those utilities to avoid tripping the relevant cybersecurity measures.[14] That bad actor also will have a good sense as to which utilities have not adopted such measures and which utilities, as a result, might be softer targets. Further, even though under the proposed PQ List approach, "any cybersecurity expenditure that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive,"[15] the NOPR provides that a utility's request for incentive-based rate treatment "must include a detailed explanation of how the utility plans to implement one or both of the proposed incentive approaches and the requested rate treatment."[16] Consolidating incentive applications that contain sensitive information in one location (the Commission's eLibrary) may increase the overall risk to the BES. If information about proposed (and implemented) cybersecurity enhancements for BES Cyber Systems is on file with the Commission, a bad actor need only focus its efforts on one location to access this critical information rather than on each individual utility.

However, NRECA agrees that, to the extent that Commission decides to maintain a public PQ List, it should update the PQ List by adding, removing, or modifying eligible cybersecurity

---

[14] NRECA does not take a position on whether the Commission should include internal network security monitoring ("INSM") on the initial PQ List, but notes that INSM can increase the attack surface. As a result, the Commission should consider the potential ramifications if it elects to include INSM on the initial PQ List. Permitting the use of INSM on a case-by-case basis instead might be a more prudent approach. NRECA clarifies that these thoughts do not alter its position on the Commission's proposals on INSM in Docket No. RM22-3-000.

[15] *Id.* at PP 3, 26.

[16] *Id.* at P 50.

expenditures only via a rulemaking proceeding.[17] In the NOPR, the Commission acknowledges that the proposed approach "would require the Commission to review and update the PQ List on a regular basis, which introduces additional process and may delay the eligibility of cybersecurity expenditures for incentives."[18] Nonetheless, updating this PQ List only via a rulemaking proceeding will ensure that interested parties and ratepayers have the opportunity to comment on proposed revisions and their potential benefit to ratepayers and national security.

If the Commission decides to adopt the case-by-case approach over the PQ List approach, NRECA requests that the Commission establish either specific project screening criteria or minimum levels of benefits utilities will need to demonstrate that their cybersecurity expenditures meet to be eligible for the requested incentive-based rate treatment. Establishing specific project criteria or minimum levels of resultant benefits will ensure cybersecurity upgrades result in tangible and measurable cybersecurity benefits. NRECA also requests that the Commission establish a process to confirm that the cybersecurity expenditure had the effects described in the application after the utility has implemented it. This process should address how the Commission will evaluate the impact of the cybersecurity expenditure and confirm that it had no unintended negative consequences. The process also should address the frequency with which the Commission reevaluate the cybersecurity expenditure (*e.g.*, annually during the life of the incentive) and whether continued eligibility for the incentive-based rate treatment would be contingent upon project completion and evaluation of the impact/risks mitigated.

---

[17] *Id.* at P 31.

[18] *Id.* at P 27.

B. PROPOSED RATE INCENTIVES FOR CYBERSECURITY INVESTMENTS

NRECA appreciates the Commission's proposal to provide for a variety of approaches for cybersecurity investments.[19] NRECA, however, requests that the Commission reconsider its proposal to specify that public utilities may request a ROE adder of 200 basis points and instead consider revising section 35.48(e)(1) to allow for a request of ***up to*** 200-basis points. While the Commission proposes to offer other incentives for cybersecurity investment, including the ability to seek deferred cost recovery in the form of regulatory assets[20] and performance-based rate treatments that reward utilities for achieving stated goals,[21] NRECA questions whether it is appropriate to grant the same ROE adder for all cybersecurity expenditures or whether the Commission instead should tie the amount of the ROE incentive to the projected impact of the cybersecurity expenditure. This is consistent with NRECA's request that the Commission specify criteria or otherwise establish a minimum level of benefit or value that cybersecurity expenditures must provide to overall grid security or reliability. In other words, NRECA asks that the Commission consider tailoring ROE adders to the impact a proposed cybersecurity investment would have on the retail and wholesale customers of that utility and overall grid security. Tying the level of the ROE adder to the benefit level or value of the proposal will help ensure that the costs to the ratepayers are commensurate with the benefits received.

C. APPLICATION PROCESS AND IMPLEMENTATION

NRECA requests that the Commission include more detailed guidance concerning both the application process and the planned implementation in any final rule. First, it would be valuable

---

19 *Id.* at P 33.

20 *Id.* at PP 33, 39-43.

21 *Id.* at PP 44-45.

for the Commission to provide insight into the information and materials that should be included with any application. Under the NOPR, the Commission states that "a request must include a detailed explanation of how the utility plans to implement one or both of the proposed incentive approaches and the requested rate treatment" as well as "detail on the expenditures for which [the utilities] seek incentives, and show how [the utilities'] cybersecurity-related expenditure(s) meet the eligibility requirements."[22] For utilities seeking incentive-based rate treatment under the PQ List approach, the Commission explains that the applicant "must provide evidence that the utility has made one or more pre-qualified cybersecurity expenditures and otherwise complies with all appropriate requirements."[23] For utilities seeking incentive-based rate treatment under the case-by-case approach, however, the Commission provides no insight into its expectations for the contents of the filing. The Commission also does not include any specific requirements for performance-based incentives in section 35.48(g) of the Commission's regulations. NRECA requests that the Commission propose language addressing applications under the case-by-case approach as well as language specifying the criteria for applications for performance-based incentives.

Second, it would be helpful for the Commission to describe the anticipated composition of teams responsible for reviewing and evaluating requests under the proposed new provisions. Given the wide-ranging implications of granting cybersecurity incentives, the reviewing team should include staff with diverse backgrounds, including electrical engineers who understand the structure of the transmission and generations assets that may be affected by the proposed cybersecurity

[22] *Id.* at P 50.

[23] *Id.* at P 52.

investment, system or computer science engineers who understand the nature of the proposed investments, and analysts with ratemaking experience who can balance the increase benefits of the proposed investment against the cost to the ratepayers.

Third, the Commission should consider whether and how it would confirm that cybersecurity expenditures had the effects described in the application. In its comments in Docket Nos. AD20-19 and RM21-3, NRECA queried how the Commission would evaluate the impact of a proposed project and would confirm that the project had the effects described in the application but no unintended consequences. NRECA also queried how frequently the Commission would reevaluate the project (*e.g.*, annually during the life of the incentive). In the NOPR, the Commission proposes that recipients of incentives would submit annual informational filings with the Commission.[24] In NRECA's experience, this places a large burden on the ratepayers to review and analyze the information provided. This is particularly true where the incentive-based rate treatment flows through a formula rate and interested parties must trace the relevant information through the formula rate and ensure the accuracy of formulas applying different ROEs, especially where certain of those ROEs are capped. NRECA requests that in addition to the information the Commission has stated must be included in those annual informational filings, the Commission also require that the annual informational filings include any changes to the categorization of any incentivized enhancements and affirmatively state that the previously incentivized enhancement remains valid. NRECA also asks that the Commission consider issuing responses confirming the continued applicability of incentive rate treatment in response to the annual informational filings.

[24] *Id.* at PP 55-56.

Finally, NRECA is concerned that because of the need to protect the confidentiality of cybersecurity systems and protocols, applications submitted under the proposed provisions will not be sufficiently transparent for interested parties to conduct effective reviews during the Commission's traditional comment period. This concern is two-fold. On the one hand, NRECA agrees that permitting applicants to submit information under the Commission's confidential and Critical Energy/Electric Infrastructure Information (CEII) filing regulations[25] is necessary. For example, sharing information concerning the geographic location of investments likely would present unnecessary risks in exchange for transparency. Further, as noted above, consolidating incentive applications that contain sensitive information in one location (the Commission's eLibrary) may increase the overall risk to the BES. However, on the other hand, the more information that applicants are permitted to mask from the public, the greater the burden placed on interested parties. The Commission should carefully evaluate and provide clear guidance on what information should be included with an application and what information may be marked as confidential or CEII in any final rule.

[25] *Id.* at P 24.

IV. CONCLUSION

WHEREFORE, NRECA respectfully requests that the Commission consider its comments as it evaluates a potential new framework for providing transmission incentives to utilities for cybersecurity investments.

Respectfully submitted,

NATIONAL RURAL ELECTRIC
COOPERATIVE ASSOCIATION

/s/ Mary Ann Ralls
Mary Ann Ralls
Senior Regulatory Counsel

National Rural Electric Cooperative
Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5837

THOMPSON COBURN LLP

/s/ Jesse Halpern
Jesse Halpern

1909 K Street, N.W.
Suite 600
Washington, DC 20006
Telephone: (202) 585-6900

Counsel for National Rural Electric Cooperative Association

November 7, 2022