UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

CYBERSECURITY INCENTIVES POLICY WHITEPAPER	**DOCKET NO. AD20-19-000**

COMMENTS OF THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

The National Rural Electric Cooperative Association ("NRECA") respectfully submits comments in response to the Cybersecurity Incentives Policy White Paper published by the Federal Energy Regulatory Commission ("Commission") Staff in this docket on June 18, 2020.[1] The White Paper explores a potential new framework for providing transmission rate incentives to utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the Critical Infrastructure Protection ("CIP") Reliability Standards. NRECA appreciates the opportunity to submit comments on the Commission Staff's White Paper 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 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

[1] *Cybersecurity Incentives Policy White Paper*, Notice of White Paper, Docket No AD20-19-000 (issued June 18, 2020) ("White Paper").

farming communities, electric cooperatives power 1 in 8 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 834 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 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.

---

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

[3] 16 U.S.C. § 824o (2018).

Barry R. Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5781
Email: barry.lawson@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 understands and appreciates Commission Staff's desire to explore ways in which to augment the current CIP Reliability Standards under Federal Power Act ("FPA") section 215 with an incentive-based approach under FPA section 219 that encourages utilities to undertake cybersecurity investments on a voluntary basis. However, after reviewing the frameworks outlined in the White Paper, NRECA requests that the Commission exercise caution if it elects to move forward in implementing incentives for cybersecurity investments.

1. Should the Commission consider adopting one or both of the CIP Reliability Standards and NIST Framework approaches? Describe any other possible approach in detail.

NRECA is concerned that the approaches outlined in the White Paper will not achieve desired results. Under the first approach, the White Paper suggests that "the Commission could provide a utility [a return on equity ("ROE")] adder or other incentive for voluntarily applying certain CIP Reliability Standards to facilities that are not currently subject to those requirements."[4] This approach envisions utilities applying the CIP Reliability Standards "requirements for medium (or high) impact systems to low impact systems, and/or the requirements for high impact systems to medium impact systems."[5] Under the second approach, the White Paper suggests that the

[4] White Paper at 15.

[5] *Id.*

Commission would "consider the CIP Reliability Standards as a basis for granting cybersecurity incentives, while allowing utilities to employ alternative approaches to assessing risk under the National Institute for Standards and Technology ('NIST') Cybersecurity Framework."[6]

In creating incentives for utilities to apply certain CIP Reliability Standards requirements to facilities that are not currently subject to those requirements, the Commission may inadvertently encourage utilities to divert resources from protecting high and medium impact BES Cyber Systems. This is because utilities have finite resources and, absent this proposed approach, a utility is likely to evaluate the risks on its transmission system and use the funds and other resources earmarked for reliability purposes to reduce their greatest risks. By contrast, under this proposed approach, utilities would be encouraged to direct their finite resources to applying CIP Reliability Standards requirements to a facility that might have little or no effect on the overall reliability and security of the Bulk Electric System simply because the utility would be able to earn a greater ROE. This approach does not take into consideration whether an investment would reduce the overall risk to the Bulk Electric System.

Further, in tying the incentives to investments in cybersecurity, the proposed approaches 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 approaches encourage utilities to make investments on which they can earn a ROE and not to address their greatest risks. In some cases, however, 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 a ROE adder incents investment

[6] *Id.* at 18.

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. Are the methods for granting incentives based on the CIP Reliability Standards (Med/High and Hub-Spoke Method) adequate? What steps should the Commission consider taking to ensure the incentive eligibility and corresponding application evaluation processes are clear and fair? What other types of cybersecurity investment based on the CIP Reliability Standards should be eligible for the incentive? Describe in detail the other types of cybersecurity investment based on the CIP Reliability Standards and how they would enhance cybersecurity.

If the Commission determines it is appropriate to implement a framework for granting cybersecurity incentives, regardless of whether that framework is based on the CIP Reliability Standards or the NIST Framework, there are several areas the Commission should explore in greater depth in addition to those outlined in the White Paper. See the response to question 4 below for more detail.

3. Should the Commission provide a rebuttable presumption of the reasonableness and thus the applicability of incentives for some or all investments in either the Med/High or the Hub-Spoke Method?

If the Commission determines it is appropriate to implement a framework for granting cybersecurity incentives, it should not provide a rebuttable presumption of reasonableness for some or all investments. The Commission should evaluate each proposed project to ascertain the value the proposed project would provide to customers and grid operations. If the Commission does not specify criteria or otherwise establish a minimum level of benefit or value that projects must provide to overall grid security or reliability, the incentive 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.

Further, as part of the project-by-project evaluation criteria, the Commission also should establish how utilities are permitted to capture the ongoing costs for those projects for which the Commission grants an incentive. For example, if an entity upgrades a low impact substation to incorporate medium impact BES Cyber System security controls, would the incentive cover the cost of the upgrade only or also the ongoing costs of operating and maintaining the enhanced security controls? Moreover, if the incentive ROE adders are flowing through formula rates on a project-by-project basis, how will the Commission track the overall cost/rate impacts and determine whether those rate impacts are just and reasonable?

4. Is the proposed approach for granting incentives based on the NIST Framework adequate? What steps should the Commission consider taking to ensure the incentive eligibility and corresponding application evaluation processes are clear and fair? What type of incentive would encourage cybersecurity improvements based on the NIST Framework? Should the incentives be available to incremental cybersecurity measures applied to both operational technology and corporate network information technology systems?

If the Commission determines it is appropriate to implement a framework for granting cybersecurity incentives, regardless of whether that framework is based on the CIP Reliability Standards or the NIST Framework, there are several areas the Commission should explore in greater depth in addition to those outlined in the White Paper. First, the Commission should consider who would be responsible for evaluating the proposed investments. This includes the background and experience of the person(s) evaluating the request. For example, would the reviewer have an electrical engineering or computer science/engineering background or ratemaking background? Would the reviewer be a Commission employee, a NERC or Regional Entity employee, or some combination? Would the reviewer have hands-on experience operating a utility's cybersecurity program or a theoretical background?

Second, the Commission should consider how it would evaluate the potential benefits of a proposed project. For example, would the Commission grant greater incentives for projects that enhance the reliability and security of high or medium BES Cyber Systems as compared to low impact BES Cyber Systems? Would the Commission review one-line or network diagrams? Would the Commission require a study or expert testimony detailing the anticipated effects of the project? Would the Commission quantify the benefits associated with a project? Would the Commission require that the benefits of a project extend beyond the utility proposing the project to surrounding utilities?

Third, the Commission should consider how it would determine the appropriate ROE adder for a project. In the White Paper, Commission Staff queried whether a 200-basis point adder would be sufficient to incent investment. The Commission also should consider whether it is appropriate to grant the same ROE adder for all projects or whether it should tie the amount of the ROE incentive to the projected impact of the project.

Fourth, the Commission should consider whether and how it would confirm that the project had the effects described in the application after the utility has implemented it. For example, how would the Commission evaluate the impact of the project? How will the Commission confirm that the project had the effects described in the application but no unintended consequences? How frequently will the Commission reevaluate the project (*e.g.*, annually during the life of the incentive)? Who would conduct the evaluation? Would the incentives be contingent upon project completion and evaluation of the impact/risks mitigated? Would the Commission assess a penalty where an entity failed to complete a project (possibly due to changing Reliability Standards, resource constraints, etc.)?

7. Is a 200-basis point project-specific ROE adder enough to materially incent cybersecurity investments that exceed the requirements of the CIP Reliability Standards? If not, what size basis point ROE incentive adder would be adequate to incentivize such cybersecurity investments? If project-specific ROE adders are not sufficient, are there other approaches that the Commission could take with respect to ROE adders that would incent the desired cybersecurity investments?

If the Commission determines it is appropriate to implement a framework for granting cybersecurity incentives, the Commission should consider forms of incentive other than ROE adders. First, as noted in response to question 1 above, an incentive in the form of a ROE adder encourages utilities to make investments on which they can earn a ROE. However, a more efficient means of enhancing the security of BES Cyber Systems might be hiring additional staff or contracting with an outside entity with specialized expertise and experience. A project-specific ROE adder, regardless of size, would not incent this type of investment.

Second, ROE adders are relevant only to Commission-jurisdictional utilities. As a result, they are not designed to incentivize cybersecurity enhancements by the vast majority of cooperatives or other non-jurisdictional utilities. Because both jurisdictional and non-jurisdictional utilities are subject to the Reliability Standards and responsible for grid security and reliability, NRECA recommends that the Commission instead collaborate with the Rural Utilities Service and the Department of Energy to identify and jointly develop other types of incentives or assistance programs to encourage cybersecurity program enhancements. The use of non-ROE-based incentives would better ensure uniformity and a more consistent approach to grid investment across the BES.

Third, because both jurisdictional and non-jurisdictional utilities are subject to the Reliability Standards and responsible for grid security and reliability, the Commission's proposed

approach of granting ROE adders as incentives could result in a "patchwork" of enhanced security measures and rate increases that disproportionately impact transmission-dependent utilities, including cooperatives and other smaller, non-jurisdictional utilities.

Finally, if the Commission determines that granting incentive ROE adders is appropriate, the Commission should consider tying the size of the ROE adder to the value to the customer of the proposed cybersecurity enhancement. In other words, the Commission should tailor incentive ROE adders to the impact a proposed project would have on the retail and wholesale customers of that utility and overall grid security. For example, it would not be just and reasonable for the Commission to grant a utility an incentive ROE adder for a project that would enhance the cybersecurity of a facility that could go down, but with no impacts on BES security and/or reliability.

9. Would the documentation requirements of the two approaches described above require disclosure of confidential information or CEII or would applicants be able to make the suggested showings without disclosing confidential information or CEII? If so, would the requirement to provide this information subject to disclosure to intervenors under a protective agreement discourage applications for cybersecurity incentives?

If the Commission determines that one-line or network diagrams are necessary to evaluate incentive applications, it should conduct a thorough review of its data protection policies and options. First, utilities must comply with Reliability Standard CIP-011. If the Commission were to require the submission of sensitive one-line and network diagrams as part of an incentive application, how would it handle the constraints of Reliability Standard CIP-011?

Second, 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.

11. Given the rapidly changing cybersecurity environment, should the Commission adopt a sunset date of three to five years for certain incentivized cybersecurity investments? At what point in the timeline between NERC announcing that it is exploring a new standard and final Commission approval, should the Commission no longer accept new applications for incentives for such investments?

The Commission should impose a sunset provision on any incentive granted to limit the incentive period to the shortest time frame possible. In determining the appropriate length of the incentive period, the Commission should evaluate several issues. First, will the Commission tie the incentive period to the measurable, verifiable benefits to retail and wholesale customers? If so, how will the Commission determine the appropriate incentive period? Second, how will the Commission confirm that the proposed project will provide those benefits for the full incentive period? Third, will the Commission re-evaluate whether a project is providing the measurable, verifiable benefits to retail and wholesale customers at regular intervals during the incentive period? If so, how?

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/ Barry R. Lawson
Barry R. Lawson
Senior Director, Regulatory Affairs

National Rural Electric Cooperative
Association
4301 Wilson Boulevard
Arlington, VA 22203
Telephone: (703) 907-5781

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

August 17, 2020