UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Policy White Paper	Docket No. AD20-19-000

COMMENTS OF THE TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to respond to the Commission staff's Cybersecurity Incentives Policy White Paper.[1] TAPS supports the goal of continuing to secure the grid against cyber threats. As transmission dependent utilities ("TDUs"), TAPS members pay, through transmission rates, for investments made by other utilities to improve their transmission facilities' cybersecurity. TAPS members also make investments, without any additional financial incentives, to secure their own assets. TAPS therefore supports investments in transmission cybersecurity that are prudent and effective. Transmission owners already have ample financial incentive to make those investments. TAPS therefore does not support granting new ROE incentives for cybersecurity investments, unless doing so can be shown to benefit consumers and result in just and reasonable rates.

The White Paper's proposal will not achieve that objective. Instead, it will increase consumer costs without necessarily providing any new security benefits. The Commission should therefore not pursue the policy proposed in the White Paper. If the Commission does, nevertheless, grant incentives for cybersecurity investments, several

[1] *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19-000 (Jun. 18, 2020), eLibrary No. 20200618-4003 ("White Paper").

changes and clarifications are need to the White Paper's proposal to ensure the incentive complies with the requirements of Federal Power Act section 219.

I. INTEREST OF TAPS

TAPS is an association of TDUs in more than thirty-five states promoting open and non-discriminatory transmission access.[2] Representing entities entirely or predominantly dependent on transmission facilities owned and controlled by others, TAPS has long recognized the need for reliable and secure transmission infrastructure that enables TAPS members to serve their load affordably. As TDUs, TAPS members make investments to secure their own assets and pay, through transmission rates, for investments made by other utilities to improve their transmission facilities' security. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards, including the Critical Infrastructure Protection ("CIP") standards.

In addition to participating at NERC and before the Commission on policy matters related to cybersecurity, TAPS has participated actively in numerous Commission proceedings concerning transmission incentive policies, including those underlying Order 679, the 2012 Policy Statement, the 2019 Notice of Inquiry on transmission incentives, and the Commission's recent Notice of Proposed Rulemaking in Docket No. RM20-10-00. TAPS has supported use of risk-reducing incentives, rather than cost-increasing incentives.

[2] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

Communications regarding these proceedings should be directed to:

John Twitty
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
PO Box 14364
Springfield, MO 65814
(417) 838-8576
Email: jtwitty@tapsgroup.org

Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
Email: cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

II. COMMENTS

A. New ROE Incentives are not needed to induce prudent and appropriate cybersecurity investments.[3]

The Commission should not adopt new ROE incentives for transmission owners that make investments in cybersecurity above and beyond what is required by mandatory standards. The Commission's recovery policies already make such projects attractive, low-risk investments.

As Chairman Chatterjee noted at the March 2019 technical conference on security investments, the Commission "has been very accommodating in providing a number of mechanisms for utilities to recover the costs of their prudently incurred security expenditures."[4] Widespread adoption of formula rates combined with the Commission's "presum[ption] that all expenditures are prudent"[5] significantly reduces the risk that TOs will not recover costs related to improving reliability and security beyond what is required by mandatory standards. Commissioner Glick's conclusion at the end of that

[3] This section responds, in part, to Questions 1 and 7 in the White Paper's Request for Comments.

[4] Transcript from March 28, 2019 Technical Conference at 151:5-7, *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (Apr. 26, 2019), eLibrary No. 20190426-4001 ("Security Conference Transcript").

[5] *Potomac-Appalachian Transmission Highline, LLC*, 158 FERC ¶ 61,050, P 100 (2017).

conference was that "cost recovery at the state or federal level really isn't a barrier to utilities doing what they need to do to protect . . . from physical or cyberattacks."[6]

Investors have confirmed that investing in grid reliability is a good deal. Nick Atkins, CEO of AEP, stated that investments in resiliency and reliability of the grid are "really probably one of [the] least risky investments we can make."[7] And Exelon "believes that the Commission's existing policies and mechanisms reasonably allow owners and operators of energy infrastructure to recover the costs of their physical and cyber security investments."[8] Edison Electric Institute ("EEI") estimates that electric utilities have invested $285 billion in transmission and distribution since 2012 to harden the grid and make it more resilient.[9] That trend will continue, with EEI estimating that a significant portion of electric company transmission spending in the future will be devoted to improving resilience and security.[10]

The White Paper acknowledges that the "ability to automatically recover prudently incurred investments in transmission infrastructure security as they are incurred provides a significant incentive for utilities to make such investments."[11] Yet the White Paper never explains why that existing "significant incentive" is inadequate to support the

---

[6] Security Conference Transcript at 187:22-24; *see also id.* at 78:17 (regulators typically allow recovery of costs associated with resiliency and reliability of the grid); *id.* at 151:14-16 (Exelon's six utilities "have not experienced any issues with recovery on the prudent investments around the physical and cybersecurity.").

[7] Security Conference Transcript at 78:18-19.

[8] Post-Technical Conference Comments of Exelon Corporation at 1, *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (May 28, 2019), eLibrary No. 20190528-5161 ("Exelon Comments").

[9] EEI, *Smarter Energy Infrastructure: The Critical Role and Value of Electric Transmission*, 3 (Mar. 2019), https://www.eei.org/issuesandpolicy/transmission/Documents/2018%20Smarter%20Energy%20Infrastructure%20The%20Critical%20Role%20and%20Value%20of%20Electric%20Transmission.pdf.

[10] *Id.* at 5.

[11] White Paper at 8.

desired level of investment. In fact, the White Paper asserts—in discussing the need for investment—that utilities should "have the ability to make cybersecurity investments to quickly and effectively adapt to address unforeseen circumstances,"[12] but then ignores the fact that existing rate structures already give transmission owners *exactly that ability*.

The White Paper also ignores evidence, submitted in response to the March 2019 technical conference, demonstrating that transmission owners are already making above-and-beyond cybersecurity investments using the current cost recovery mechanisms. For example, Dominion asserted that its strong safety culture drives its companies "to make the necessary investments in security infrastructure, oftentimes above and beyond what is minimally required by mandatory standards or industry guidelines."[13] And Exelon explained that its companies "are taking initiatives that are not addressed by or go above reliability and security standards when appropriate and prudent."[14]

Faced with evidence that existing cost recovery mechanisms are incentivizing the desired above-and-beyond investments, the White Paper's premise crumbles. Rational decision making requires an answer to a basic question: Why are additional financial incentives needed? Without a more thorough analysis of the existing level of investment, the desired level of investment, and the barriers preventing the desired level, the Commission cannot answer that question.

---

[12] *Id*. at 12.

[13] Post-Technical Conference Comments of Dominion Energy Services, Inc. at 2, *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (May 28, 2019), eLibrary No. 20190528-5159.

[14] Exelon Comments at 29; *see also id.* 12-13 (describing plans to mitigate vulnerabilities "that, while not severe enough to violate NERC or other reliability standards, could significantly disrupt service to our customers.").

The White Paper's logical flaw is exemplified by its question of whether "a 200-basis point project-specific ROE adder [is] enough to materially incent cybersecurity investments."[15] Without evidence of what level of investment is needed and why the existing rate recovery mechanisms are inadequate to achieve that, the Commission cannot rationally determine what level of incentive is "enough."

B. Transmission Owners must not receive incentives for investments that they would otherwise make.[16]

If, despite a lack of need for them, the Commission proceeds with a proposal to grant cybersecurity incentives, modifications are needed to the White Paper's approach. One basic modification is a clarification that transmission owners must not be eligible for cybersecurity incentives for investments they would otherwise have made. The Commission staff in the White Paper and the Commission itself in its recent Notice of Proposed Rulemaking have already acknowledged that incentives are not appropriate for maintaining an adequate level of reliability.[17] Certainly, that means that transmission owners may not receive incentives for complying with NERC CIP Standards, but the principle extends further in the context of cybersecurity.

First, some utilities have agreed as part of a NERC mitigation plan to make certain investments that go above and beyond the requirements of the NERC CIP Standards. Those are financial commitments made in consideration for reduced penalties for past violations. A transmission owner who has made such commitments cannot be allowed to request incentive treatment for those investments.

---

[15] White Paper at 27.

[16] This section responds, in part, to Questions 2, 4, 5 and 8 in the White Paper's Request for Comments.

[17] White Paper at 3; Incentives NOPR, P 64.

Second, transmission owners cannot be granted incentives for actions or investments required by state regulators. States have their own requirements and programs for cybersecurity, and most of the utility's costs for cybersecurity on state-jurisdictional assets shows up in the utility's IT budget;[18] a transmission owner cannot be allowed to seek incentives from the Commission for cybersecurity investments on its distribution system or corporate IT system, if those investments were made pursuant to state requirements.

Third, and perhaps most importantly, the White Paper proposal for granting incentives based on the NIST Framework is an open invitation to transmission owners to re-package their existing plans into an incentive application. As noted above, there is evidence that utilities are already making investments that go above and beyond NERC's requirements.[19] Because the NIST Framework is not prescriptive and allows entities flexibility in how to implement and customize its practices,[20] it would be easy for a utility to re-characterize its pre-existing, planned, cybersecurity investments as belonging to one of the Framework's five functions, twenty-three categories, and 108 subcategories. Granting incentives for activities that would have happened anyway is not only bad

[18] Statement of Commissioner Chivukula, *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (April 2, 2019), eLibrary No. 20190402-4015 ("A recent unpublished survey of 22 PUCs by NRRI supports NREL's findings that most cyber costs show up as part of IT budgets.").

[19] *See* n. 13-14 above.

[20] NIST Framework, at vi ("Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework.").

policy, but also contradictory to Section 219's requirements that incentives "benefit consumers" and result in just and reasonable rates.[21]

The ease by which incentives based on the NIST Framework can be gamed is reason enough not to grant incentives based on that framework. So too is the inherent intractability in verifying compliance with the NIST Framework. The very nature of the NIST Framework—a flexible, voluntary tool that allows for customization based on specific circumstances—is simultaneously what makes it so appropriate for addressing evolving cyber threats and what makes it so inappropriate for regulatory purposes. If the Commission does adopt incentives based on the NIST Framework, despite the problems with it, the Commission must put in place safeguards to prevent transmission owners from using that incentive for projects that would have been built anyway.

C. The portion of investments used for NERC compliance or other regulatory or contractual requirements must be subtracted from any ROE incentive.[22]

As discussed above, it would be contrary to the Federal Power Act to grant incentives for investments that are required to comply with NERC requirements, other regulatory requirements, or other commitments. The corollary of that principle is that when an investment is made in part to comply with an obligation and in part to go above and beyond, any incentive should not be applied to the cost of the compliance portion.

Thus, if the Commission proposes a cybersecurity incentive at all (despite the good reasons for not doing so), it should account for investments, for example, that are simultaneously used for CIP compliance and for above-and-beyond cybersecurity. A

---

[21] 16 U.S.C. § 824s.

[22] This section responds, in part, to Question 6 in the White Paper's Request for Comments.

transmission owner seeking an incentive for such an investment must reveal the portion of the investment being used for CIP compliance, and may only seek the incentive on the incremental costs above that required for CIP compliance.

D. Given the diversity of systems, configurations, and investments, it would be inappropriate to rebuttably presume that voluntarily applying certain CIP Reliability Standards to lower impact BES Cyber Systems will produce significant benefits.[23]

Compared to medium and high impact BES Cyber Systems, low impact BES Cyber Systems encompass a much greater diversity of asset types. While CIP-002-5.1a enumerates a list of assets associated with medium and high impact BES Cyber Systems, the low impact category is a catchall, including all BES Cyber Systems not included as medium or high impact.[24] Given the diversity of systems and configurations of low impact BES Cyber Systems, NERC and the Commission have quite rightly allowed registered entities flexibility in how to achieve security goals for low impact BES Cyber Systems. For example, when NERC first proposed expanding the CIP standards to include low impact BES Cyber Systems, which until then had not been subject to any standards, it explained that "overriding concern was that by mandating specific controls, the Reliability Standards would ultimately stunt the development of the range of controls necessary to protect the diversity of Low Impact assets now subject to the CIP Reliability Standards."[25]

---

[23] This section responds, in part, to Question 3 in the White Paper's Request for Comments.

[24] NERC, CIP-002-5.1a – Cyber Security – BES Cyber System Categorization, Attachment 1.

[25] Comments of NERC on the Notice of Proposed Rulemaking for Version 5 Critical Infrastructure Protection Reliability Standards at 21, *Version 5 Critical Infrastructure Protection Reliability Standards*, Docket No. RM13-5-000 (June 24, 2013), eLibrary No. 20130624-5173.

More recently, in response to a Commission's directive related to electronic access controls for low impact BES Cyber Systems, NERC proposed modifications in CIP-003-7 that established a security objective and provided ten different conceptual frameworks for achieving that objective, recognizing that "there are many different technical solutions that can be used to implement electronic access controls" for low impact BES Cyber Systems.[26] The Commission initially proposed to direct NERC to further modify the standard to "provide clear, objective criteria for electronic access controls for low impact BES Cyber Systems," due to concerns that auditors would not be able to assess whether the solutions implemented by a utility were reasonable.[27] The Commission suggested that the standards for medium and high impact BES Cyber Systems could serve as "a possible model" for the low impact standard.[28] In the final rule, however, the Commission declined to adopt the proposed directive.[29]

The Commission implicitly recognized in that order that, while the more prescriptive controls required for medium and high impact BES Cyber Systems may be easier to audit, more flexibility is needed to ensure the security of low impact BES Cyber Systems. Given the greater diversity of the low impact BES Cyber systems, indiscriminately applying standards designed for medium and high impact BES Cyber Systems may have the opposite of the intended effect, "stunt[ing] the development of the

---

[26] Petition of NERC for Approval of Proposed Reliability Standard CIP-003-7 at 25, Docket No. RM17-11 (Mar. 3, 2017), eLibrary No. 20170303-5213.

[27] Notice of Proposed Rulemaking, *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 161 FERC ¶ 61,047 (2017).

[28] *Id.*, P 31.

[29] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 163 FERC ¶ 61,032 (2018).

range of controls necessary to protect the diversity of Low Impact" BES Cyber Systems.[30]

Thus, if the Commission considers granting any incentive for cybersecurity investments, it should not adopt the White Paper's proposal to grant a rebuttable presumption that implementing medium or high impact CIP Reliability Standards for facilities designated as low impact would provide significant benefits. A transmission owner seeking such incentives must affirmatively demonstrate that the investments it is making will indeed provide significant reliability benefits. Specifically, an applicant should be required to (1) identify the particular BES Cyber Assets to which the CIP standards will be applied, (2) demonstrate how the application of the CIP standards to particular lower impact assets will result in significant cybersecurity benefits for Commission-jurisdictional transmission facilities,[31] (3) identify quantifiable metrics for the expected enhanced cybersecurity benefits,[32] (4) identify the investments that have been or will be made to achieve those benefits, and (5) demonstrate that the ROE incentive is needed to induce the identified investment.

E. Transmission customers must have an opportunity to evaluate any incentive requests.[33]

Determining whether a particular cybersecurity incentive is necessary and that the investment induced by that incentive will produce significant benefits to consumers is

---

[30] NERC, *supra*, note 25.

[31] *Cf.* White Paper at 22 (requiring applicants for incentives based on the NIST Framework to show, among other things, how the investments "resulted in significant cybersecurity benefits for Commission-jurisdictional transmission facilities").

[32] *Cf. id.* at 25 (proposing to require applicants to "submit quantifiable metrics to support that the expected enhanced cybersecurity benefits were realized.").

[33] This section responds, in part, to Question 9 in the White Paper's Request for Comments.

necessarily a fact-and assumption-specific endeavor. Such incentive applications must be scrutinized in formal proceedings that provide the Commission and intervenors with access to the information and modeling necessary to evaluate, reproduce, and contest the applicant's benefit claims. Information access is crucial for intervenors to meaningfully participate in proceedings where the Commission evaluates those claims.

In many cases, the information needed to scrutinize cybersecurity incentive applications will include CEII. Customer scrutiny should not, however, be limited because of the need to protect and limit dissemination of the CEII. The Commission's existing CEII regulations have worked in a wide range of Commission proceedings, and they can be made to work for cybersecurity incentive applications too, provided that adequate time and procedures are put in place for transmission customers to obtain and review the necessary information.

Specifically, any cybersecurity incentive application will require a meaningful opportunity for evidentiary hearings (with ample time for discovery) to avoid arbitrary determinations and unjust and unreasonable rates. The fundamental FPA requirement that rates be just and reasonable cannot be satisfied by a process that effectively forecloses objection. Nor can material issues of fact be decided on the basis of pleadings.

In short, the Commission's CEII regulations can and must be used to limit dissemination of any CEII that is included in an incentive application, but those same regulations should not be used as a shield for utilities to avoid scrutiny of their rates.

F. Any ROE adders should be limited in time, subject to the cap on total ROE incentives, and not granted for cost overruns.[34]

If, despite the good reasons for not doing so, the Commission adopts new ROE adders for cybersecurity investments, those adders must be limited consistent with Section 219's requirement that incentives be just and reasonable. Specifically, any ROE adder should be (1) limited to three years, (2) included in a utility's cap on total ROE, and (3) limited to the budgeted investment amounts.

First, the White Paper is correct in limiting the duration of any ROE incentive for cybersecurity investments.[35] The White Paper acknowledges the rapidly changing nature of cyber threats;[36] the necessary implication is that investments made to protect systems may not provide the same level of security benefits five years from now. The short depreciation life of BES Cyber Systems reflects that reality. Therefore ROE incentives should last no longer than any benefits that accrue to customers from a cybersecurity investment, which is reasonably estimated to be three years.

Second, any ROE adders should be included in the cap on ROE adders that is determined by the Commission's general policy on transmission incentives. TAPS has urged the Commission to adopt a fixed cap of 100 basis points on project specific-adders and retain the cap on total ROE within the zone of reasonableness.[37] Although the ROE adders proposed in this White Paper are distinct from the ones proposed in the Commission's Incentives NOPR, the principles of capping ROE adders is embedded in

---

[34] This section responds, in part, to Question 11 in the White Paper's Request for Comments.

[35] White Paper at 27.

[36] *Id.* at 12.

[37] Comments of TAPS at 95, Docket No. RM20-10-000 (July 1, 2020), eLibrary No. 20200701-5410.

Section 219's requirement for just and reasonable rates, and therefore must apply equally to the cybersecurity incentive adders.

Finally, the Commission's 2012 Policy Statement affirmatively required that ROE incentives should be limited to budgeted amounts.[38] Any cybersecurity incentive should abide by that policy. Otherwise, applicants will have carte blanche to increase their incentive profits by allowing (or even encouraging) cost overruns. That would not be just and reasonable.

CONCLUSION

For the reasons stated above, the Commission should not adopt any new incentives for cybersecurity investments or, at minimum, should make necessary modifications to the White Paper's proposal as discussed herein.

[38] *Promoting Transmission Investment Through Pricing Reform*, 141 FERC ¶ 61,129, P 28 (2012); s*ee also PJM Interconnection, L.L.C.,* 155 FERC ¶ 61,097, P 86 (2016), *on reh'g*, 158 FERC ¶ 61,060 (2017) ("an applicant is expected to commit to limit the application of such incentive ROE adder to a cost estimate").

Respectfully submitted,

/s/ Cynthia S. Bogorad

Cynthia S. Bogorad
Latif M. Nurani

Attorneys for
Transmission Access Policy Study Group

Law Offices of:
Spiegel & McDiarmid LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 879-4000

August 17, 2020