UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	)	Docket No. RM21-3-000

REPLY COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION AND THE TRANSMISSION ACCESS POLICY STUDY GROUP

The initial comments filed by the American Public Power Association ("APPA") and the Transmission Access Policy Study Group ("TAPS") urged the Federal Energy Regulatory Commission ("Commission" or "FERC") not to adopt the incentive rate proposals included in the Notice of Proposed Rulemaking ("NOPR") issued in the above-captioned proceeding.[1] APPA and TAPS each also suggested certain modifications and clarifications to the NOPR should the Commission proceed with the proposed rule. Taken as a whole, these initial comments show that the proposed rule would not result in just and reasonable rates to consumers, and the Commission should certainly not adopt the suggestions of some commenters to *expand* the already generous cybersecurity incentives proposed in the NOPR – or to weaken the proposed application and verification procedures.

I. REPLY COMMENTS

A. The Initial Comments Show that Incentives are Not Needed

APPA and TAPS argued in their initial comments that incentives are not needed to promote prudent cybersecurity investment, and, therefore, the incentive framework proposed in the NOPR would not result in just and reasonable rates.[2] The initial comments (including some filed by incentive proponents) confirm that public utilities are already incentivized to make

[1] *Cybersecurity Incentives*, 173 FERC ¶ 61,240 (2020), 86 Fed. Reg. 8309 (Feb. 5, 2021).

[2] *See* APPA Comments at 14-17; TAPS Comments at 5-8. *See also, e.g.*, *City of Detroit v. FPC*, 230 F.2d 810, 817 (D.C. Cir. 1955) (explaining that there must be a showing that the incentive "is in fact needed, and is no more than is needed, for the purpose.").

prudent cybersecurity investments beyond those required to comply with North American Electric Reliability Corporation ("NERC") mandatory Critical Infrastructure Protection ("CIP") reliability standards, even in the absence of Commission-awarded incentives.[3] Disregarding the specific inquiry of Chairman Glick and Commissioner Danly,[4] the proponents of incentives never explain why incentives are actually *needed* to promote prudent cybersecurity investment, and, indeed, they generally ignore the legal standards for incentive rates altogether. At most, their comments make nebulous assertions that incentives would give cybersecurity investments a leg up in the "internal competition for capital resources."[5] Such undocumented claims cannot support a finding of need, particularly given the record of investment without incentives and the availability of existing cost recovery mechanisms for prudent cybersecurity expenditures.[6]

[3] *See, e.g.*, Edison Electric Institute ("EEI") Comments at 3 ("The industry's multi-layered approach to protecting the energy grid encompasses compliance with NERC Reliability Standards, as well as activities that surpass the minimum requirements of the standards."); *id.* at 4 ("EEI members are already making investments that go beyond NERC's Reliability Standards, as appropriate."); Electric Power Supply Association ("EPSA") Comments at 3 ("competitive suppliers routinely exceed what is required by standards and regulations"); International Transmission Company d/b/a ITC*Transmission*, et al. ("ITC") Comments at 6 ("ITC is wholly committed to making any and all prudent investments in its cybersecurity infrastructure necessary to achieve a robust level of defense, and conversely, has no interest in deploying additional investments which are not already warranted merely to achieve a slightly higher level of return."); Midcontinent ISO Transmission Owners ("MISO TOs") Comments at 5 ("the MISO Transmission Owners already make voluntary cybersecurity investments far in excess of the CIP Reliability Standards"); *see also* California Department of Water Resources State Water Project ("CDWR") and California Public Utilities Commission ("CPUC") Comments at 4-7 (identifying cybersecurity investments by California public utilities); NERC Comments at 4-5 (providing "examples of the ERO Enterprise approach to improving the cybersecurity posture of entities through mechanisms above and beyond Reliability Standards alone.").

[4] NOPR, Chairman Glick and Comm'r Danly Concurrence at P 3 ("We encourage commenters to address whether—and, if so, why—additional measures, such as an elevated ROE or deferred cost recovery, are necessary to incentivize public utilities to adopt additional cybersecurity measures.").

[5] PJM Transmission Owners ("PJM TOs") Comments at 7.

[6] *See* APPA Comments at 14-17; TAPS Comments at 5-8; *see also, e.g.*, CDWR/CPUC Comments at 4-5 (discussing federal and state cost recovery mechanisms); Organization of MISO States ("OMS") Comments at 4 ("The OMS strongly supports enhanced cybersecurity, but there is no record of state and local regulators refusing cost recovery for utilities reacting aggressively and responsibly to quell cybersecurity threats.").

B. The Initial Comments Document Concerns that Incentives Could Divert Resources Away from Other Prudent Cybersecurity Investments

APPA and TAPS expressed concern that the NOPR framework could actually diminish cybersecurity by encouraging public utilities to invest in measures that are eligible for incentives rather than in the most effective cybersecurity enhancements.[7] The comments of incentive proponents reinforce these concerns by enumerating various investments and activities that they think should be eligible for incentives beyond those proposed in the NOPR.[8] The opportunity to invest in these other measures tends to show that the NOPR's proposal to incentivize "automated and continuous monitoring" under the National Institute of Standards and Technology ("NIST") Cybersecurity Framework Approach and the CIP Incentives Approach could detract from other, potentially more effective, cybersecurity investments. Indeed, ITC argues that the CIP Incentives Approach "runs directly contrary to the risk-based methods at the core of many entities' cybersecurity plans, which seek to focus resources and efforts on truly High Impact BES Cyber Assets to achieve appropriate proportionality between the risks involved and costs of various security measures."[9] The solution is not to incentivize any and all cybersecurity investments (as the utilities would prefer). The better approach is to recognize that no incentives are needed to make prudent investments and that it could be counterproductive to promote a particular subset of investments.

---

[7] *See* APPA Comments at 13-14; TAPS Comments at 8; *see also* National Rural Electric Cooperative Association Comments at 5.

[8] *See, e.g.*, EEI Comments at 4 (seeking flexibility on approaches); *id.* at 9-10 (all NIST controls should be eligible); Hitachi ABB Power Grids ("Hitachi") Comments at 2 (incentives for physical security and security assessments); ITC Comments at 2-3 (describing alternate standards that should be eligible); *id.* at 4 (other NIST controls should be eligible); MISO TOs Comments at 7-8 (all NIST controls); PJM TOs Comments at 10-11 (any "new and innovative cybersecurity projects"); *id.* at 8-9 (all NIST categories).

[9] ITC Comments at 2-3; *see also id.* at 8.

C. The Commission Should Reject Calls for Broader or Even More Lucrative Incentives

If the Commission proceeds with the incentive framework described in the NOPR, it should reject requests from some commenters to expand the investments eligible for incentives or to make the proposed incentives even more lucrative.

Two commenters, for example, suggest the Commission should allow utilities to collect the return on equity adder incentive ("ROE Adder") on amounts deferred for recovery under the Regulatory Asset Incentive.[10] They make no showing that double incentives are needed to induce a company to spend money on cybersecurity expenses like training. The Commission correctly concluded that granting both incentives for the same expenditures "is unnecessary to incent investment."[11] ITC confirms that the Regulatory Asset Incentive, without an additional ROE adder, would be sufficient to promote investment in cybersecurity infrastructure.[12]

The Commission should likewise dismiss the PJM TOs' request that FERC allow the ROE Adder to exceed the zone of reasonableness.[13] As Commissioner Christie recently explained in his concurrence to the supplemental notice of proposed rulemaking in Docket No. RM20-10, the Commission should be skeptical of the use of ROE adders absent specific statutory authorization (lacking here), because "by definition, an ROE adder raises the cost of capital *above* the market cost, inflicting on consumers exactly the harm that utility regulation is supposed to prevent."[14] An incentive ROE above the top end of the zone of reasonableness

[10] EEI Comments at 11-12; PJM TOs Comments at 15.

[11] NOPR at P 38.

[12] ITC Comments at 6-7. APPA and TAPS do not believe that the Regulatory Asset Incentive is needed to incent investment. APPA Comments at 19; TAPS Comments at 9.

[13] PJM TOs Comments at 12-13.

[14] *Elec. Transmission Incentives Policy Under Sec. 219 of the Federal Power Act*, 175 FERC ¶ 61,035, Comm'r Christie Concurrence at P 10 (2021).

would not bear any relationship to the market cost of capital and would fail to satisfy the Federal Power Act's ("FPA") just and reasonable rate requirement.[15]

Nor should the Commission adopt proposals to expand the investments or processes eligible for incentives.[16] Commission Staff correctly recognized in the White Paper that an incentive framework must include "an approach for identifying the cybersecurity investments that [FERC] seeks to incentivize."[17] An incentive program that allows public utilities to request incentives for adopting miscellaneous NIST Framework controls or "new, innovative cybersecurity projects" that a public utility asserts "will provide significant cybersecurity benefits to the transmission system"[18] does not clearly identify which investments are eligible for incentives. Such an approach would increase the likelihood that public utilities would seek incentives for routine cybersecurity measures that are simply good utility practice, which would be contrary to the principle that incentive rates should be understandable for customers.[19] Similarly, it would be unreasonable to allow broad categories of traditional expense items to be

[15] *See Emera Maine v. FERC*, 854 F.3d 9, 23 (D.C. Cir. 2017) (noting "[t]he zone of reasonableness informs FERC's selection of a just and reasonable rate."); *Me. Pub. Utils. Comm'n v. FERC*, 454 F.3d 278, 288 (D.C. Cir. 2006) (upholding incentive adder for participation in ISO New England based, in part, on application of a zone of reasonableness cap).

[16] *See, e.g.*, EEI Comments at 9-10 (proposing to expand the NIST Framework incentive to all five categories of security controls and related training); *id*. at 11-12 (expressing concern with the Commission's proposal not to allow O&M costs to be capitalized and added to rate base with a 200-basis point adder); Hitachi Comments (proposing to expand the NOPR to physical security, as well as security assessments and costs for lifecycle support for eligible investments); MISO TOs Comments at 10 (proposing to expand the universe of investments eligible for incentives); PJM TOs Comments at 8-10 (proposing to expand the categories of security controls incentivized under the NIST Framework); *id*. at 15 (proposing to increase the cost categories eligible for Regulatory Asset Incentive treatment); SCRM Filing Parties Comments at 1 (proposing to expand NIST Framework eligibility to software supply chain risk management products, processes, and procedural improvements).

[17] Cybersecurity Incentives Policy White Paper, Docket No. AD20-19-000 at 14 (June 2020).

[18] PJM TOs Comments at 10.

[19] *See* TAPS Comments at 4, 17-18 (citing *Incentive Ratemaking for Interstate Nat. Gas Pipelines, Oil Pipelines, & Elec. Utils.*, 61 FERC ¶ 61,168, at 61,590 (1992) (stating that an incentive mechanism must "be understood by all parties" and that the net "benefits to consumers must be quantifiable")).

capitalized whenever a public utility can claim some nexus to cybersecurity.[20] Such rate treatment is particularly unnecessary and unreasonable given that public utilities are essentially assured full and timely recovery of prudent expenses through transmission formula rates.

D. Utilities are Not Entitled to Incentives that No Longer Serve Their Intended Purpose

It would be unjust and unreasonable to adopt the request of some commenters to allow incentives to remain in effect even after the relevant cybersecurity investments have become mandatory.[21] The Commission may only award incentives that are *needed* to encourage particular actions or investments.[22] If an investment is required to comply with the CIP Reliability Standards, an incentive is, by definition, no longer needed. Customers should not be required to bear the extra ongoing costs of incentives on mandatory investments based simply on when a utility made the investment. As APPA explained in its initial comments, the Commission should adopt an even earlier cut-off for cybersecurity incentives than proposed in the NOPR.[23] Among other benefits, APPA's proposed approach would partially mitigate fears

[20] *Cf.*, *Dow Corning Corp.*, 59 FERC ¶ 61,191, at p. 61,666 (1992) ("The accounting rules . . . are not construed on the basis of whether they will provide proper incentives or disincentives. The purpose of these rules is to accurately, consistently and neutrally portray the financial performance of regulated companies. . . . If an exception were allowed to these rules whenever a party cited a possible incentive or disincentive, the rules would no longer serve their purpose of properly depicting financial performance.").

[21] *See* EEI Comments at 14; MISO TOs Comments at 12.

[22] *See City of Detroit*, 230 F.2d at 817; *Cal. Pub. Utils. Comm'n v. FERC*, 879 F.3d 966, 975 (9th Cir. 2018) (observing that "[a]n incentive cannot 'induce' behavior that is already legally mandated. Thus, the voluntariness of a utility's membership in a transmission organization is logically relevant to whether it is eligible for an adder.").

[23] APPA argued that the cut-off for incentives for extending the CIP Standards requirements to lower risk assets should be the earlier of: (1) the date of any Commission directive under FPA section 215 that would require increasing the requirements for a low or medium impact system to those of a medium or high impact system; or (2) the date a Standards Authorization Request that would require an increase in the requirements for a low or medium impact system to those of a medium or high impact system is submitted to the NERC Standards Committee. *See* APPA Comments at 23-24.

that utilities might seek to delay reasonable new standards to continue collecting incentives on "voluntary" investments – a concern also raised by NERC in its comments.[24]

The Commission should also dismiss ITC's suggestion that the Commission allow regulatory asset treatment for recovery of obsolete or ineffective prior cybersecurity investments that are being replaced.[25] Customers should not be forced to pay for the amortization (with a return) of non-used and useful cybersecurity investments. Moreover, as the NOPR observes cybersecurity investments generally have short lifespans and high depreciation rates,[26] making it unlikely that utilities frequently will be faced with the prospect of having to write off these investments due to obsolescence.

Finally, there can be no merit in the argument that utilities should be authorized to continue benefitting from cybersecurity incentives even when they fail to implement the measures for which the incentive has been granted.[27] The alleged difficulty in tracking compliance is not a basis for charging customers full price for diminished benefit,[28] nor should utilities get a pass for "minor" deviations from the incentive requirements.[29] As beneficiaries of proposed incentives under FPA section 205, utilities have the burden to show that any incentive rate proposals are just and reasonable, including assurance of compliance with the terms of any proposal. In any case, the NOPR does not propose to penalize utilities for non-compliance;

---

[24] *See id.* at 14; NERC Comments at 9 ("While the ERO Enterprise appreciates the Commission's efforts to encourage industry to adopt stronger practices voluntarily, the ERO Enterprise is concerned that it may create financial reasons to oppose the standards development process.").

[25] ITC Comments at 7.

[26] NOPR at PP 46, 59.

[27] *See* EEI Comments at 6-8; PJM TOs Comments at 25-28.

[28] *See* EEI Comments at 7; PJM TOs Comments at 26.

[29] EEI Comments at 6-7 (arguing that in these so-called "minor" cases, the "impact of non-conformance to the CIP Reliability Standard does not warrant complete ineligibility for the incentive"); PJM TOs Comments at 27-28 (requesting that the Commission "find that minor or administrative and other minimal risk instances of non-compliance would not result in the suspension of an incentive.").

utilities would still be entitled to recover the costs of cybersecurity investments, they simply would not be entitled to earn incentives when they fail to satisfy the applicable requirements. The NOPR's proposal is already inappropriately generous because utilities' opportunities for reward are not offset by a symmetric downside risk.[30] Making it even more generous by replacing the *opportunity* for reward with a *guaranteed* reward regardless of a utility's compliance would be plainly unjust and unreasonable.

E. The Commission Should Not Apply a Rebuttable Presumption of Benefit to Either of the Proposed Cybersecurity Approaches

APPA's and TAPS' initial comments urged the Commission not to apply a rebuttable presumption that investments under the NERC CIP Incentives Approach materially enhance cybersecurity.[31] APPA and TAPS both argued that such a presumption was unwarranted, and, given the information asymmetry between utilities and their customers concerning cybersecurity systems and processes, APPA contended that the presumption may be effectively irrebuttable.[32]

For the same reasons, APPA and TAPS urge the Commission to reject calls from some commenters to apply a rebuttable presumption to the NIST Framework Approach.[33] Additionally, it would be even less warranted to grant a rebuttable presumption for the NIST Framework Approach because of the wide variety of ways in which a utility could implement those controls. Whether an investment made under the NIST Framework Approach will materially enhance security is, necessarily, a case-by-case determination.[34] Thus, as with the

[30] *See* TAPS Comments at 22-23 (explaining that the proposal's lack of serious penalties for non-compliance undermines compliance and is contrary to the Incentive Policy Statement, which requires section 205 incentives be symmetrical).

[31] APPA Comments at 19-20; TAPS Comments at 12-17.

[32] APPA Comments at 19-20.

[33] *See* EEI Comments at 10; MISO TOs Comments at 11; PJM TOs Comments at 10.

[34] APPA Comments at 12-13; TAPS Comments at 19.

CIP Incentives Approach, it would not be just and reasonable simply to presume that use of the NIST Framework Approach will result in material cybersecurity benefits. ITC's comments highlight the issue, arguing that the test for incentives "should not simply be whether it checks a different box, but whether the investment will meaningfully address specific underlying cybersecurity risks and vulnerabilities. The NERC CIP Incentives Approach may do so, but it is no more likely to than the NIST Framework Approach."[35] ITC's diagnosis of the problem is correct; its cure is incorrect. The solution is not to give all investments a rebuttable presumption; it is to give no rebuttable presumptions.

F. The Need to Protect CEII Should Not Be Used to Deny Access to Customers that Would be Paying for Incentives

APPA and TAPS recognize the importance of protecting Critical Energy/Electric Infrastructure Information ("CEII") and agree that CEII must be adequately shielded in the application and auditing processes for cybersecurity incentives. The need to protect CEII from unwarranted disclosure, however, should not be a basis to deny transmission customers and other interested parties a meaningful opportunity to evaluate the merits of a cybersecurity incentive application or a utility's compliance with an order awarding such incentives. Accordingly, the Commission should reject proposals from some commenters to limit (or even eliminate) the information that utilities must include in initial incentive applications or subsequent informational filings.[36]

[35] ITC Comments at 8.

[36] *See* EEI Comments at 10; ITC Comments at 5-6; PJM TOs Comments at 16. Notably, MISO TOs "do not object to the proposed initial 120-day post-completion reporting requirement for cybersecurity upgrades receiving incentive treatment." MISO TOs Comments at 13. Nor do the MISO TOs "object to the idea of an annual reporting requirement detailing the specific investments that were made pursuant to the Commission's approval, and what FERC Accounts they fall into." *Id.*

Review of CEII must be subject to appropriate confidentiality restrictions, but it is not possible to determine if a rate is just and reasonable without knowing how the money being charged is being spent. Providing evidence that a utility has done what it was paid an incentive to do is not unduly burdensome; it is a reasonable obligation in response to receiving a significant financial benefit. Moreover, the information the utilities are trying to protect is already discoverable in their rate proceedings or formula rate update processes, subject to appropriate confidentiality mechanisms, and there is no reason to scale back the information requirements proposed in the NOPR.[37]

G. Competitive Suppliers Should Not Be Eligible for Incentives

The Commission should reject EPSA's suggestion that the Commission allow generators with market-based rates to receive the proposed cybersecurity incentives.[38] As a threshold matter, awarding incentives to competitive suppliers under the kind of framework outlined in EPSA's comments would not represent a "logical outgrowth" of the NOPR, and, thus, could not be properly included in any final rule.[39] Further, as EPSA argues in its comments, competitive suppliers already "routinely exceed what is required by standards and regulations,"[40] and granting competitive suppliers cost recovery for such cybersecurity investments could distort the competitive energy and ancillary services markets.[41]

---

[37] The Commission should also reject EEI's suggestion that the Commission allow capitalization of traditional expense items on a self-implementing basis. *See* EEI Comments at 13. In Order No. 679, the Commission rejected calls for automatic or self-implementing incentives, and it should abide by that policy here. *See Promoting Transmission Investment through Pricing Reform*, Order No. 679, 116 FERC ¶ 61,057, at PP 68, 80, 82, *order on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *order on reh'g*, 119 FERC ¶ 61,062 (2007).

[38] EPSA Comments at 5-6.

[39] *See, e.g.*, *CSX Transp., Inc. v. STB*, 584 F.3d 1076, 1079-81 (D.C. Cir. 2009); *Data Collection for Analytics and Surveillance and Market-Based Rate Purposes*, 170 FERC ¶ 61,129, at P 10 & n.22 (2020).

[40] EPSA Comments at 3.

[41] *See* TAPS Comments at 20.

II. CONCLUSION

APPA and TAPS appreciate the opportunity to provide these reply comments on the NOPR. APPA and TAPS respectfully submit that the incentive program proposed in the NOPR is not necessary or appropriate to promote cost-effective and prudent public utility investment in cybersecurity measures. If the Commission adopts a final rule in this proceeding, the Commission should reject the expansions and modifications suggested by various commenters, as discussed above.

Respectfully submitted,

/s/ John E. McCaffrey
Delia Patterson
Senior Vice President, Advocacy and
Communications and General Counsel
John E. McCaffrey
Senior Regulatory Counsel
American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

/s/ Cynthia S. Bogorad
Cynthia S. Bogorad
Latif M. Nurani
Anree G. Little*
Spiegel & McDiarmid LLP
1875 Eye Street, NW Suite 700
Washington, DC 20006
(202) 879-4000

Attorneys for
Transmission Access Policy Study Group

Dated: May 6, 2021

* Admitted to the Maryland Bar and not currently admitted to practice in D.C. His work is supervised by principals of the firm pursuant to D.C. App. R. 49(c)(8).