UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF
TRANSMISSION ACCESS POLICY STUDY GROUP

The Transmission Access Policy Study Group ("TAPS") appreciates the opportunity to comment on the Commission's September 22, 2022 Notice of Proposed Rulemaking ("NOPR").[1]

TAPS recognizes the importance of protecting the grid from cyber attacks through mandatory North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Standards and through prudent, cost-effective, and voluntary investments that go above and beyond the requirements of those standards. TAPS believes that the Commission's existing rate recovery structures provide adequate incentives for public utilities to make those voluntary investments. Nevertheless, TAPS acknowledges that the Commission is required by Federal Power Act section 219A[2] to establish incentive-based rate treatments to encourage cybersecurity investments and participation in information sharing programs.

FPA section 219A has the purpose of benefitting consumers both by encouraging investment in technology that will enhance the security of public utilities, and by ensuring

---

[1] *Incentives for Advanced Cybersecurity Investments*, 180 FERC ¶ 61,189 (2022) ("NOPR").

[2] 16 U.S.C. § 824s-1(a).

that the resulting rates are just and reasonable.[3] TAPS appreciates that the NOPR takes positive steps towards balancing those two goals; but further revisions are needed to adequately protect consumers from unjust and unreasonable incentive rates. The lodestar for determining whether an incentive rate is just and reasonable is that the incentive is "in fact needed, and is no more than is needed, for the purpose."[4] Adhering to that requirement, TAPS suggests the following modifications to the NOPR's proposal:

- The Commission should adopt the PQ List approach, not the case-by-case approach, but should commit to regularly reviewing the PQ List for continued eligibility. *See* Section II.A.

- The Commission should expand the definition of "mandated" cybersecurity investments to include investments made to satisfy *any* legal obligation; and utilities should be required to attest that requested incentives are not mandated. *See* Section II.B.

- Modifications are needed to the proposed incentive mechanisms to make them just and reasonable, including: (1) reducing the ROE Incentive adder; (2) limiting the ROE Incentive duration to a maximum of 3 years; (3) limiting the Regulatory Asset Incentive to 50% of incentive-eligible expenses for 5 years; (4) eliminating the sunset exemption for the incentive for information sharing programs; and (5) combining the above reductions with high impact, low cost non-financial incentives. *See* Section II.C.

- Customers must have a meaningful opportunity to evaluate and meaningfully respond to any incentive requests. *See* Section II.D.

- The Commission should explicitly exclude generators with market-based rates from incentive eligibility. *See* Section II.E.

---

[3] 16 U.S.C. § 824s-1(c) (incentive rate treatment must "benefit[] consumers by encouraging—(1) investments by public utilities in advanced cybersecurity technology"); 16 U.S.C. § 824s-1(e)(1) (Resulting incentive rates "shall be subject to the requirements of sections 824d and 824e of this title that all rates, charges, terms, and conditions—(A) shall be just and reasonable; and (B) shall not be unduly discriminatory or preferential.").

[4] *City of Detroit v. Fed. Power Comm'n*, 230 F.2d 810, 817 (1955).

I. INTEREST OF TAPS

TAPS is an association of transmission-dependent utilities ("TDUs") in more than thirty-five states promoting open and non-discriminatory transmission access.[5] 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 CIP standards. In addition to participating at NERC and before the Commission on policy matters related to cybersecurity, including the 2021 Notice of Proposed Rulemaking on Cybersecurity Incentives in Docket No. RM21-3,[6] TAPS has participated actively in numerous other Commission proceedings concerning transmission incentive policies, including those underlying Order No. 679,[7] the 2012 Policy Statement,[8] the 2019 Notice of Inquiry on

---

[5] Jane Cirrincione, Northern California Power Agency, is TAPS Chair. Dave Osburn, Oklahoma Municipal Power Authority, is Vice Chair. Terry Huval is TAPS Executive Director.

[6] *Cybersecurity Incentives*, 173 FERC ¶ 61,240 (2020), *terminated by*, *Incentives for Advanced Cybersecurity Investment*, 180 FERC ¶ 61,189 (2022).

[7] *Promoting Transmission Investment through Pricing Reform*, Order No. 679, 116 FERC ¶ 61,057, *on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *clarified*, 119 FERC ¶ 61,062 (2007) ("Order No. 679").

[8] *Promoting Transmission Investment Through Pricing Reform*, 141 FERC ¶ 61,129 (2012).

transmission incentives,[9] and the Commission's Notice of Proposed Rulemaking in Docket No. RM20-10.[10]

Communications regarding these proceedings should be directed to:

Terry J. Huval
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
P.O. Box 60551
Lafayette, LA 70596
(337) 278-0306
Email: thuval@tapsgroup.org

Cynthia S. Bogorad
Anree G. Little
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
Email: cynthia.bogorad@spiegelmcd.com
anree.little@spiegelmcd.com

II. COMMENTS

A. The PQ List approach, with certain modifications, will balance the objectives of encouraging investment and protecting ratepayers; the case-by-case approach will not.

The NOPR proposes to establish a list of pre-qualified expenditures that would be presumed to be eligible for an incentive (the "PQ List"). A utility seeking an incentive would still need to make an individualized filing to demonstrate that its expenditures qualify as being associated with an item on the PQ List and that the resulting rates are just and reasonable. The NOPR proposes to initially include two specific expenditures—internal network security monitoring and participation in the Department of Energy Cybersecurity Risk Information Sharing Program ("CRISP")—on the PQ List, with the expectation that items will be added and removed from the PQ List through notice-and-

---

[9] *Inquiry Regarding the Comm'n's Elec. Transmission Incentives Pol'y*, 166 FERC ¶ 61,208 (2019).

[10] *Elec. Transmission Incentives Pol'y Under Section 219 of the Fed. Power Act*, 170 FERC ¶ 61,204, *errata notice*, 171 FERC ¶ 61,072 (2020).

comment rulemaking. The Commission could initiate such a rulemaking *sua sponte* or in response to a petition.

TAPS generally supports the PQ List approach. Modifying the list by rule will improve regulatory certainty for utilities and customers. It will also better facilitate participation and input on whether a particular type of expenditure meets the eligibility criteria of (a) materially improving cybersecurity, and (b) not being already mandated. And since the Commission, utilities, and other stakeholders can propose new technologies to be added to the PQ List, there is little risk that worthy, voluntary advanced cybersecurity technologies will be overlooked.

To make the PQ List more effective at achieving Section 219A's goals, the Commission should modify the proposed PQ List approach as described below.

1. Each item on the PQ List should be regularly reviewed for continued eligibility.

Every time the Commission initiates a rulemaking proceeding to consider adding an item to the PQ List, the Commission should review each item already on that list to ensure each continues to meet the eligibility criteria. TAPS urges the Commission codify this essential task in the final regulatory text adopted in this proceeding.

It would not be just and reasonable, nor would it "benefit consumers,"[11] to maintain items on the PQ List that no longer materially improve cybersecurity. Just as cyber threats evolve rapidly, the availability and quality of the technologies developed in response also rapidly evolve.[12] It is therefore necessary for the Commission to regularly reaffirm that

---

[11] *See* FPA section 219A(c), 16 U.S.C. § 824s-1(c).

[12] *See* NOPR P 31 (noting the "rapidly evolving nature of cybersecurity threats and solutions").

each item on the PQ List continues to be an *advanced* cybersecurity technology that will benefit consumers by enhancing the security posture of utilities.[13]

A commitment to review and reaffirm that each item on the PQ List meets the eligibility criteria will facilitate the Commission's obligation to ensure mandated technologies do not receive incentives.[14] As the NOPR correctly notes, "if a cybersecurity expenditure on the PQ List becomes mandatory, it would no longer be eligible for an incentive as of the effective date of the mandate."[15] Similarly, when use of an advanced cybersecurity technology becomes, over time, widespread in the industry, that technology may be considered Good Utility Practice,[16] and therefore no longer worthy of an incentive.[17]

While the NOPR expects the Commission to "regularly evaluate the PQ List and update it,"[18] without an express obligation to review each item on the PQ List there is a risk that once-advanced technologies will remain on the list well after they are no longer truly advanced. Regular re-evaluation of each item on the list will benefit consumers by helping to ensure the PQ List continues to be targeted, effective, and worthy of incentives.

---

[13] An alternative approach could be to have items automatically removed from the PQ List after a certain period of time (e.g., 3-5 years), absent an affirmative finding by the Commission that the item continues to satisfy the eligibility criteria.

[14] See discussion in Section II.B below on better defining the scope of technologies that should be considered mandatory.

[15] NOPR P 31.

[16] The Commission's *pro forma* OATT defines Good Utility Practice as "[a]ny of the practices, methods and acts engaged in or approved by a significant portion of the electric utility industry during the relevant time period." § 1.15.

[17] A cybersecurity expenditure that is Good Utility Practice clearly should not be eligible for addition to the PQ List.

[18] *Id*. P 31.

2. The Commission should not adopt a case-by-case approach to evaluate an investment's eligibility for incentive treatment.

As an alternative to the PQ List approach, the NOPR seeks comment on whether a utility's cybersecurity expenditure should be evaluated on a case-by-case basis to determine if such expenditure satisfies the eligibility criteria for incentive treatment, including whether that the expenditure is voluntary and materially improves cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program.[19]

TAPS strongly urges the Commission *not* to adopt a case-by-case approach. A case-by-case approach would not accomplish the Commission's objectives because it would reduce regulatory certainty, increase litigation expense, and slow down adoption of advanced cybersecurity technologies.

First, with "no presumption of eligibility for any given cybersecurity expenditure,"[20] each applicant would bear the full burden to demonstrate that its cybersecurity expenditure meets the Commission-approved eligibility criteria, leaving considerable regulatory uncertainty surrounding every application. Moreover, the breadth of technology options encompassed by the six sources identified by the NOPR[21] opens up virtually unlimited possible combinations of technology investments that could be proposed by each utility in the 1,669-member applicant pool.[22] For example, the National

---

[19] NOPR P 32.

[20] *Id*.

[21] *Id*. P 21.

[22] *Id*. P 71 ("The NERC Compliance Registry, as of August 5, 2022, identifies approximately 1,669 utilities, both public and non-public, in the U.S. that would be eligible for this proposed incentive and rate treatment.").

Institute of Standards and Technology ("NIST") Framework is a comprehensive and flexible catalog of system and organization security and privacy control objectives in twenty different categories,[23] which exist "independent of the process employed to select those controls."[24] Similarly, the Cybersecurity Capability Maturity Model contains more than 350 cybersecurity practices in ten different domains.[25] Because there is essentially no limit to the technologies that could be proposed under these six cybersecurity frameworks, utilities will have little (if any) certainty about whether a particular technology will be approved under the case-by-case approach.

Second, a case-by-case approach would be administratively inefficient for the Commission and participants in the incentive application proceeding. Each application would require a fact-intensive analysis into particularly sensitive aspects of the utility's security posture. Evaluating the first prong of the eligibility criteria, i.e., whether the investment "would materially improve cybersecurity,"[26] involves a fact-specific inquiry into the utility's existing attributes, its system configuration, the specific characteristics of the investment, and more. The second eligibility criterion (i.e. voluntariness) could be equally burdensome to administer under the case-by-case approach, because unlike the PQ

---

[23] *See* NIST, *Security and Privacy Controls for Information Systems and Organizations* (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (access control; awareness and training; audit and accountability; assessment, authorization, and monitoring; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; program management; personnel security; personally identifiable information processing and transparency; risk assessment; system and services acquisition; system and communications protection; system and information integrity; and supply chain risk management).

[24] *Id.* at 3 (page 30 of pdf).

[25] U.S. Dep't of Energy, Cybersecurity Capability Maturity Model (C2M2), https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[26] NOPR P 28.

List approach in which the Commission would have a discrete list of technologies to assess for voluntariness, the case-by-case approach would require an individualized determination for each possible technology to determine whether it is explicitly or implicitly mandated by a CIP Reliability Standard or some other legal obligation. This could prove difficult, particularly for the public, especially given CEII restrictions.

Finally, the case-by-case approach would slow down adoption of advanced cybersecurity technologies. The NOPR expresses concern that the PQ List approach would "introduce[] additional process and may delay the eligibility of cybersecurity expenditures for incentives."[27] But adding new technologies to the PQ List by rule will, in many cases, be faster than individualized, case-by-case adjudications that are set for evidentiary hearings to ascertain whether the utility has met its burden to demonstrate the eligibility criteria are met.

B. The NOPR correctly recognizes that incentives cannot be given for investments a utility is obligated to undertake; but the scope of mandated investments should be expanded.

The Commission's longstanding policy, incorporated in Order No. 679[28] and recognized by the courts,[29] is that rate incentives are prospective and that there must be a connection between the incentive and the conduct meant to be induced. This core requirement for incentive rates to be just and reasonable prohibits the Commission from "rewarding utilities for past conduct or for conduct which they are otherwise obligated to

---

[27] *Id.* P 27.

[28] Order No. 679, P 26.

[29] *Cal. Pub. Utilities Comm'n v. FERC*, 879 F.3d 966, 977 (9th Cir. 2018).

undertake."[30] FPA section 219A incorporates that longstanding requirement through its "Ratepayer Protection" clause.[31]

The NOPR seeks to implement that requirement by proposing that a cybersecurity investment will not be eligible for an incentive if the investment is mandated by an enforceable CIP Reliability Standard or by local, state, or Federal law.[32] That eligibility criteria has twin functions: (1) it generically prevents technologies from being added to the PQ List if those technologies are already mandated,[33] and (2) it specifically prevents a utility from receiving an incentive for an expenditure on the PQ List if the expenditure is mandated *for that utility*.[34]

TAPS applauds that eligibility criteria as a good first step, but it is not sufficient to achieve the objective of limiting incentives to voluntary actions. Further revisions are necessary to ensure incentive rates are just and reasonable.

---

[30] See, e.g., *Dayton Power & Light Co.*, 176 FERC ¶ 61,025, P 30 (2021) (quoting *Cal. Pub. Utils. Comm'n v. FERC*, 879 F.3d 966, 977 (9th Cir. 2018)). The Commission then reiterated: "Consistent with that longstanding policy, we do not believe it would be appropriate to award an incentive for an action that the requesting entity is required by law to take." *Id*.

[31] FPA section 219A(e)(1), 16 U.S.C. § 824s-1(e)(1) (Incentive rates are "subject to the requirements of [FPA] sections [205 and 206] . . . that all rates, charges, terms, and conditions— (A) shall be just and reasonable.").

[32] NOPR P 20.

[33] *Id.* P 31 ("The eligibility criteria described above . . . would guide the Commission's decision on what to add, modify, or remove from the PQ List . . . if a cybersecurity expenditure on the PQ List becomes mandatory, it would no longer be eligible for an incentive.").

[34] *Id.* P 26 (Intervening parties can rebut the PQ List presumption by demonstrating "that, given the unique circumstances of the utility, the expenditure for which the utility seeks an incentive . . . is otherwise mandatory for that utility.").

1. The definition of "mandated" cybersecurity investments should be expanded to include investments made to satisfy *any* legal obligation.

The proposal fails to recognize that a utility's legal obligations go beyond CIP Reliability Standards, or local, state, or Federal law. A utility may also have legal obligations to make cybersecurity investments pursuant to state or federal regulatory proceedings, state or federal enforcement proceedings, settlement agreements, or other contracts. For example, a utility may be required to make cybersecurity investments as:

- A remedial measure as a settlement of past NERC compliance violations.[35]
- A condition of a state or federal license.[36]
- A condition of a merger proceeding.[37]
- An obligation under its cybersecurity insurance policy.[38]

---

[35] *See, e.g.*, NERC, Notice of Penalty Unidentified Registered Entity 5, Docket No. NP18-7-000 (Feb. 28, 2018), eLibrary No. 20180228-5108 (Settlement Agreement approved by the NERC Board of Trustees Compliance Committee resolving an alleged violation of CIP-003-3 requiring protection of information associated with Critical Cyber Assets, including a $2.8 million fine, several corrective actions and mitigations, including investments to deploy "a suite program to provide policies and controls to prevent confidential-Bulk Electric System (BES) Cyber System Information or restricted-BES Cyber System Information classified emails and attachments from being sent to outside email addresses" and "requiring vendors to take information security and privacy awareness training annually, implementing a new vendor remote access platform, and enhancing policies, background checks, and contract language for vendor employees.").

[36] *See, e.g.*, Nuclear Regulatory Commission and Federal Energy Regulatory Commission Joint Meeting, Tr. 91:25-92:4, Docket No. AD06-6-000 (Mar. 31, 2022), eLibrary 20220412-4000 (discussing implementation of an NRC rule where the cybersecurity plans that nuclear plant licensees submit become a condition of their license.).

[37] *See* NOPR P 20.

[38] A 2021 Government Accountability Office ("GAO") report found that the insurance industry has responded to increasing frequency and severity of cyberattacks with tighter terms and more exclusions. GAO, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market* (May 20, 2021), https://www.gao.gov/products/gao-21-477; *see also* Cheryl W. Munk, *Buying Cyber Insurance Gets Trickier as Attacks Proliferate, Costs Rise*, The Wall Street Journal (Aug. 8, 2022), https://www.wsj.com/articles/buying-cyber-insurance-gets-trickier-as-attacks-proliferate-costs-rise-11659951000 (discussing increased scrutiny by underwriters of insurance applicants' cybersecurity practices); *id*. ("Insurers want to have confidence that [companies] are making the right investments and are building and maintaining a robust cybersecurity program.").

Because incentives are not needed to induce behavior that the utility would already perform under its existing legal obligations, the Commission should revise the eligibility criteria to exclude from incentive eligibility any portion of investments made to satisfy *any* existing legal obligation, regardless of the source.

2. Utilities should be required to attest that incentivized expenditures are not being made to satisfy any legal obligation.

To help ensure mandatory investments and expenses are excluded from incentive rate treatment, the Commission should require applicants to certify that, after undertaking due diligence, they are not aware of a legal obligation that would be satisfied by any of the investments for which they seek incentive treatment; utilities awarded incentive treatments should make similar annual re-certifications as part of their informational filings. This is an administratively efficient process to deal with information asymmetries as the utility is in the best position to understand the full scope of its legal obligations.

When assessing whether a technology is used to comply with a NERC CIP Standard (either for addition to the PQ List or when evaluating a specific proposal), the Commission may consider a more nuanced approach, because many NERC CIP Standards set out performance requirements but do not mandate any particular technology to achieve those requirements. In such cases, the Commission should take care to grant incentives only for truly advanced technologies that clearly go above and beyond the NERC CIP Standards.

C. Modifications are needed to the incentive mechanisms to make them just and reasonable.

The Commission must satisfy the FPA's requirement that a just and reasonable incentive be "in fact needed, and is no more than is needed, for the purpose."[39] In considering how much of an incentive is needed, the Commission should observe the extent to which utilities are already making voluntary, above-and-beyond investments to improve their cybersecurity systems, supported by existing cost-recovery mechanisms and non-financial incentives. Indeed, the Commission already provides ample financial mechanisms to induce utilities to make prudent cybersecurity 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."[40] A 2019 Commission Staff White Paper notes the variety of actions the Commission has specifically taken to that end, including: widely adopting formula rates that flow through costs automatically;[41] presuming all costs are prudent; allowing security costs in stated rates; and even granting a separate, security-related surcharge to recover costs.[42] This backdrop, along with comments from utilities themselves,[43] led then-Commissioner Glick to

---

[39] *City of Detroit*, 230 F.2d at 817.

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

[41] During the open meeting on this NOPR, Commissioner Christie expressly highlighted formula rates as providing an incentive.

[42] FERC, Notice of White Paper at 9 n.26-28, *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19, (June 18, 2020), eLibrary No. 20200618-4003 (citing *Extraordinary Expenditures Necessary to Safeguard Nat'l Energy Supplies*, 96 FERC ¶ 61,299, at 62,129 (2001); *Boston Edison*, 109 FERC ¶ 61,300, P 40 (2004); *Policy Statement on Matters Related to Bulk Power Sys. Reliability*, 107 FERC ¶ 61,052 (2004)).

[43] *See, e.g.*, Exelon, Post Technical Conference Comments 1, *Security Investments for Energy Infrastructure Technical Conference*, Docket No. AD19-12-000 (May 28, 2019), eLibrary No. 20190528-5161 ("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.").

conclude "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."[44] Now-Chairman Glick made a similar observation at the September 22, 2022 open meeting considering this NOPR.[45]

Indeed, utilities are already making voluntary investments in advanced cyber-security absent any additional financial incentive from the Commission. For example, in its comments on the Commission's proposed rule to require NERC to develop mandatory standards for internal network security monitoring ("INSM") for high and medium impact BES Cyber Systems, Consumers Energy states it: "independently concluded that these critical systems warrant the investment in monitoring tools and infrastructure to support the added detection and forensic capability INSM provides and has already implemented INSM for most of the Company's high and medium impact BES Cyber Systems within an Electronic Security Perimeter."[46] NextEra Energy also states that it has "a comprehensive cybersecurity monitoring program for all of our computer and data networks,"[47] that "third parties periodically assess the company's alignment with the U.S. Department of Energy's Cyber Capability Maturity Model (C2M2),"[48] and that the company's "comprehensive,

---

[44] Transcript from March 28, 2019 Technical Conference at 187:22-24, *Security Investments for Energy Infrastructure Tech. Conferences*, Docket No. AD19-12-000 (Apr. 26, 2019), eLibrary No. 20190426-4001 ("Security Conference Transcript").

[45] FERC, Transcript of 1093rd Open Meeting, 37:1-13 (Sept. 22, 2022), eLibrary No. 20220923-4000 (statement of Chairman Glick).

[46] Comments of Consumers Energy Company 2, *Internal Network Security Monitoring for High and Medium Impact Bulk Elec. System Cyber Systems*, Docket No. RM22-3-000 (Mar. 28, 2022), eLibrary No. 20220328-5148.

[47] NextEra Energy, *Environmental, Social and Governance Report 2022* 58, https://www.investor.nexteraenergy.com/~/media/Files/N/NEE-IR/Sustainability/NEE_CORPORATE%20REPORT_ESG_vF.pdf (last visited Oct. 16, 2022).

[48] *Id*.

defense-in-depth approach imposes security at every layer and our standards for cybersecurity *exceed* those set by the industry."[49]

It is no surprise that utilities are making these above-and-beyond cybersecurity investments without any need for additional financial incentives. The business case for doing so is strong: it is a low-risk investment[50] that is essential to maintaining the utility's reputational value[51] and continuity of service for its customers.[52] The widespread participation in CRISP by investor-owned utilities[53] confirms that utilities are making prudent investments without additional financial incentives.

Recognizing Section 219A's directive, but accounting for the extent of voluntary activities and investment-friendly rate structures encouraging them, the additional financial inducement needed is modest. While the NOPR proposes some limits on the incentive mechanisms,[54] they remain the "FERC Candy" Commissioner Christie cautions against—sweet for those that get it, but bitter for the consumers that pay for it. Additional limitations are needed to tailor the scope and cost of the incentives to the required, modest inducement.

---

[49] *Id*. (emphasis added).

[50] Security Conference Transcript at 78:18-19 (Atkins, AEP CEO) (stating that investments in resiliency and reliability of the grid are "really probably one of [the] least risky investments we can make").

[51] Written Statement of Kevin G. Wailes of Lincoln Electric System 7, *Security Investments for Energy Infrastructure Tech. Conference*, Docket No. AD19-12-000 (Apr. 2, 2019), eLibrary No. 20190402-4009; *see also* Security Conference Transcript at 66:18-24 (Akins) ("[I]f your brand is built around operational excellence and you see it as a really something that can really diminish the brand, there's nothing worse that could happen to a company in our opinion to have a significant outage caused by any event, but let alone a cyber event.").

[52] Exelon Corp., *US Resilience Project - Best Practices in Cyber Supply Chain Risk Management*, NIST 4, https://www.nist.gov/system/files/documents/itl/csd/NIST USRP-Exelon-Case-Study.pdf.

[53] NOPR, Phillips, Comm'r, concurring P 4.

[54] For example, the NOPR already proposes that ROE incentives be capped at the top of the zone of reasonableness; both the Cybersecurity ROE Incentive ("ROE Incentive") and Regulatory Asset Incentive would be limited in duration; and utilities would not be permitted to receive both the ROE Incentive and Regulatory Asset Incentive for the same investment.

Specially, as described below, TAPS proposes (1) lowering the ROE Incentive adder; (2) limiting the ROE Incentive duration to no more than 3 years; (3) limiting the Regulatory Asset Incentive to 50% of the expenses; (4) eliminating the sunset exemption for the incentive for information sharing programs; and (5) combining these reductions with non-financial incentives.

1. A 200 basis point ROE incentive for five years will impose unnecessary cost burdens for customers.

In light of the evidence that utilities are already making prudent investments to improve cybersecurity above-and-beyond their legal obligations, there is reason to think that 200 basis points is well above the level of ROE incentive needed to induce the desired investments. The Commission should adopt a lower ROE incentive that is consistent with the level of incentives granted in the past, such as 50 basis points, before concluding (without any evidence) that a 200-basis-point adder is needed. The NOPR concedes 200 basis points is higher than what "the Commission typically provides pursuant to FPA section 219."[55] The Commission has an obligation to determine the minimum ROE that will induce the desired investment,[56] yet the NOPR contains no analysis of whether an incentive less than 200 basis points would be sufficient to induce the desired investment.

The NOPR states that "given the relatively small cost of cybersecurity investments compared to conventional transmission projects, a higher ROE may be necessary to affect the expenditure decisions of utilities, without unduly burdening ratepayers."[57] That assessment is incorrect.

---

[55] NOPR P 36.

[56] *City of Detroit*, 230 F.2d at 817.

[57] NOPR P 36.

First, the assertion that cybersecurity investments are small compared to conventional transmission projects is both unsupported and incorrect. As reflected in the Commission's order approving Duke Energy's request for special accounting treatment for its Cybersecurity Informational Technology-Operational Technology Program, Duke Energy has "ma[d]e over $137 million in capital investments as part of its Cybersecurity Program" that is "designed based on the [NIST Framework]."[58] In 2019, Dominion Energy Virginia received state approval to spend $910.3 million on Cyber and Physical Security and Telecommunications over 10 years, with $154.4 being spent in the first three years[59] related to "improved monitoring and alarm capabilities"[60] and "enhanced utility security."[61] These large sums illustrate that cybersecurity investments are not, as the NOPR states, "relatively small . . . compared to conventional transmission projects."[62] Cybersecurity investments being made outside the electricity industry (without any guaranteed cost recovery, much less financial incentives) confirm the potential magnitude:

---

[58] *Duke Energy Corp.*, 169 FERC ¶ 61,232, P 6 (2019).

[59] Final Order, *Petition of Virginia Electric and Power Company, For approval of a plan for electric distribution grid transformation projects pursuant to § 56-585.1 A 6 of the Code of Virginia*, Case No. PUR-2018-0100 (Va. State Corp. Comm. Jan. 17, 2019), https://scc.virginia.gov/docketsearch/DOCS/4dv801!.PDF.

[60] *Id* at 7.

[61] *Id*.

[62] NOPR P 36.

JP Morgan plans to invest $600 million annually; [63] Microsoft, $20 billion over the next five years;[64] and the Department of Defense, $11.2 billion in 2023 alone.[65]

Second, even if it were true that cybersecurity investments are less than major new transmission lines, there is no evidence that a higher ROE is necessary to induce such investments. In the competition within a utility for internal capital, even a small ROE incentive should be adequate to induce a utility to allocate capital towards cybersecurity investments on the PQ List. The relative size of cybersecurity investment therefore does not provide evidence that the proposed 200 basis points is "in fact needed, and no more than is needed," to encourage investment in advanced cybersecurity technology.

Given the lack of support for the necessity of 200-basis points ROE adder and the large potential cost of cybersecurity investments, the Commission should select a much lower ROE incentive to add to the already investment-supportive environment.

2. The ROE Incentive should be limited to no more than 3 years.

The ROE Incentive should be three years instead of the five years proposed in the NOPR.[66] As explained above, the incentive must be set at a level that is no higher than

---

[63] Jamie Dimon, Chairman and CEO, *Letter to Shareholders*, JP Morgan 35 (Apr. 3, 2019), https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/ceo-letter-to-shareholders-2018.pdf.

[64] NBC News, *Tech companies pledge billions in cybersecurity investments*, The Associated Press (Aug. 26, 2021), https://www.nbcnews.com/tech/tech-news/tech-companies-pledge-billions-cybersecurity-investments-rcna1784.

[65] U.S. Dep't of Defense, *The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget* (Mar. 28, 2022), https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg/.

[66] Consistent with the NOPR's proposal, the 3-year limit would be the maximum duration for the ROE Incentive. The ROE Incentive should end at the earliest of (a) 3 years, (b) the depreciable life of the underlying asset, (c) the date the investment becomes mandatory, or (d) the date the program is removed from the PQ list.

needed to induce the desired investment. The longer the duration of the ROE Incentive, the greater the total cost to ratepayers of the incentive. Reducing the incentive to three years, especially when combined with reducing its level substantially below 200 basis points, will protect consumer from unjust and unreasonable rates.

Setting the limit at 3 years better aligns with the fast-evolving nature of cybersecurity technology. Three years has the benefit of not incentivizing utilities to continue using obsolete technology just because it still gets an incentive, when an upgrade would otherwise be reasonable and appropriate.[67] Lastly, three years is consistent with the WATT/AEE's Grid Enhancing Technologies incentive proposal, which also targeted technology that can quickly evolve.[68]

3. The Regulatory Asset incentive should be limited to 50% of the expenses.

The NOPR asks whether "it would be preferable to permit only 50% of incentive-eligible expenses to be treated as regulatory assets."[69] It would. The NOPR presents no evidence that regulatory asset treatment for 100% of eligible expenses is the minimum amount needed to induce the desired expenditures. In fact, the evidence suggests the contrary. For example, most investor-owned utilities participate in CRISP even though they "only" are assured recovery of the expenses.[70] Restricting the Regulatory Asset Incentive

---

[67] *See* NOPR P 49 (noting that discrete cybersecurity investments may become obsolete with the passage of time.)

[68] *See* WATT Coalition and AEE Shared Savings Proposal, *Electric Transmission Incentives Policy*, Docket No. RM20-10-000 and *Under Section 219 of the Federal Power Act*, Docket No. AD19-19-000 (Sep. 3, 2021), eLibrary No 20210903-5088. This proposal was the subject of FERC's September 10, 2021 Workshop on Shared Savings Incentives for Transmission Technologies.

[69] NOPR P 39.

[70] *See e.g.*, NOPR, Phillips, Comm'r, concurring P 4 ("For example, 75% of electricity customers in the continental U.S. are served by investor-owned utilities that already participate in CRISP"); Exelon Post Technical Conference Comments 1, *Security Investments for Energy Infrastructure Technical Conference*,

to 50% (rather than 100%) of eligible expenses would be more consistent with the Commission's FPA obligations under *City of Detroit*.

Limiting the Regulatory Asset Incentive is also appropriate given its conflict with the Commission's traditional ratemaking principles. The Regulatory Asset Incentive allows utilities to defer recovery and treat these expenses like capital investments, recovering the expense over time along with a return. Cybersecurity expenses, like all other utility expenses, are already recoverable in the utility's yearly revenue requirement, in formula rates (and any remaining stated rates). The NOPR does not explain why a utility would prefer to "defer and amortize eligible costs"[71] over five years instead of recovering those costs immediately. If a utility's authorized rate of return closely approximates the utility's weighted average cost of capital, then the utility should be indifferent to immediate cost recovery or deferred recovery at the authorized rate of return. The effectiveness of the Regulatory Asset Incentive seems to rely on the public utility's authorized return being higher than its actual cost of capital, putting it in tension with an aim of cost-of-service regulation.

4. Participation in information sharing programs should not receive an exemption to the sunset provision.

The NOPR proposes to allow eligible expenses incurred for five years to be added to the proposed regulatory asset. TAPS agrees with the NOPR's preliminarily finding that

---

Docket No. AD19-12-000 (May 28, 2019), eLibrary No. 20190528-5161 ("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."); FERC, Transcript of 1093rd Open Meeting, 37:2-7 (Sept. 22, 2022), eLibrary No. 20220923-4000 (statement of Chairman Glick: "And as a matter of fact, we had a technical conference… I think it was 2019, where we had a bunch of utilities come before us in the technical conference and they all said we don't have a problem recovering our costs either at the federal level or at the state level.").

[71] NOPR P 39.

the five-year limit balances the goals of ratepayer protection and inducing the desired investment.[72] But the NOPR unjustifiably proposes to depart from that balance with regard to expenses incurred for eligible cybersecurity threat information sharing programs, instead allowing a perpetual incentive on those investments.[73] The Commission should not adopt such an exception for information sharing programs, because it gives no consideration of the requirement to protect ratepayers.

Once a utility takes the steps necessary to participate in an information sharing program, the incentive dynamic changes and the amount of incentive needed, if any, lowers. Economists recognize this status quo bias:[74] people prefer things to stay the same by doing nothing or by sticking with a decision made previously.[75] In terms of participation in an information sharing program, after joining, the status quo is now one of participation; the utility must now overcome that inertia and take some action to leave the program. Here, inertia works to the benefit of ratepayers and it takes less incentive, if any, to encourage the utility to continue to participate in the information program. Even if an incentive were needed to induce the initial participation, a utility is *less* likely to stop participation in the program after receiving an initial incentive, installing the advanced sensors/monitoring equipment necessary,[76] and receiving the benefits of near real-time threat information.

---

[72] *Id.* P 48.

[73] *Id.* P 49.

[74] The status quo bias has been studied in a range of fields, including Business and Economics, Information Systems, Psychology and Medicine, Politics and Law, as well as Energy and Sustainability. *See* Godefroid, ME., Plattfaut, R. & Niehaves, B., *How to measure the status quo bias? A review of current literature*, Mgmt. Rev. Q., 2 (2022), https://doi.org/10.1007/s11301-022-00283-8.

[75] Samuelson & Zeckhauser, *Status Quo Bias in Decision Making*, J. Risk & Uncertainty, 1, 7-59 (1988).

[76] CRISP participants install a passive information sharing devices (ISD) on participant networks. Dep't of Energy, *Cybersecurity Risk Information Sharing Program (CRISP)*, https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf (last visited Oct. 16,

The NOPR attempts to distinguish the ongoing nature of the expenses and benefits of information sharing program from other "discrete cybersecurity investments that may become obsolete with the passage of time."[77] That distinction, however, does not support granting a perpetual incentive for information sharing programs. The fact that participants are provided with ongoing updates after joining such programs is a recurring benefit that likely *increases* retention, absent any incentive. Indeed, the large participation in CRISP suggests utilities will participate and continue to participate, absent any Commission incentive.[78] While that may raise questions about whether any incentive is needed for utilities already participating in CRISP, it shows that—for new or existing program members—a perpetual incentive is unnecessary.

5. The Commission should complement financial incentives with low cost, high impact non-financial incentives.

Given the minimal need for and significant cost burdens created by the proposed incentives, the Commission should consider other effective, less costly options to incent utilities to go-above-and beyond in cybersecurity. For example, the Commission could publicly recognize industry excellence in cybersecurity.[79] In addition to its low-cost, public recognition offers many benefits. It provides positive examples for other utilities to model, promotes industry best practices, and doing so in cybersecurity expands the scope of efforts

---

2022).

[77] NOPR P 49.

[78] *See* NOPR, Phillips, Comm'r, concurring P 4 ("For example, 75% of electricity customers in the continental U.S. are served by investor-owned utilities that already participate in CRISP.") (citing Dep't of Energy, *Energy Sector Cybersecurity Preparedness*, https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness).

[79] It is the corollary to the negative reinforcement of publicly disclosing those that violate mandatory NERC CIP Standards.

to recognize utilities that excel in reliability in general.[80] Obviously, such a recognition program would need to protect CEII and avoid revealing sensitive security information about the winning utilities, but even sharing non-confidential information about cybersecurity innovations can spur others to adopt similar innovations. Moreover, such endorsements can stimulate competition among utilities to improve their cybersecurity posture. Today, utilities that are recognized for their cybersecurity efforts (albeit not by the Commission) feature cybersecurity strength as part of their brand, and proudly share those honors in their investor-relations publications.[81] Recognition in a Commission-sponsored forum would have an even greater impact.

Combining reduced financial incentives with non-financial incentives would be consistent with Congress's directive, and further its overarching objective to encourage investment in advanced cybersecurity technology and participation in information sharing programs. This kind of broader, more inclusive approach would also create incentives for

---

[80] *See e.g.*, San Diego Gas & Electric, *SDG&E Wins National Award for Best Electric Reliability in America, Outstanding Reliability in the West & Grid Sustainability* (Nov. 18, 2021), https://www.sdgenews.com/article/sdge-wins-national-award-best-electric-reliability-america-outstanding-reliability-west; Paul Ciampoli, *Public power utilities earn top customer satisfactions scores*, American Public Power Association (July 15, 2019), https://www.publicpower.org/periodical/article/public-power-utilities-earn-top-customer-satisfaction-scores (referencing utilities earning top rankings in J.D. Power's customer satisfaction study, driven in part by "focusing their efforts on improving reliability"); U.S. News & World Report, *Energy Rankings - Measuring States' Energy Infrastructure*, Best States Ranking, https://www.usnews.com/news/best- states/rankings/infrastructure/energy (last visited Oct. 16, 2022) (Grid reliability was one of three categories specifically ranked).

[81] *See e.g.*, NextEra Energy, Environmental, *Social and Governance Report 2022* at 59 "Awards and Recognitions" ("In 2021, FPL won the ReliabilityOne® National Reliability Excellence Award for the sixth time in the last seven years, presented by PA Consulting to the award recipient that has demonstrated sustained leadership, innovation and achievement in the area of electric reliability."), https://www.investor.nexteraenergy.com/~/media/Files/N/NEE-IR/Sustainability/NEE_CORPORATE%20REPORT_ESG_vF.pdf (last visited October 16, 2022).

small utilities that do not have a rate on file and thus are not eligible for financial incentives.[82]

D. Customers must have a meaningful opportunity to evaluate and meaningfully respond to any incentive requests.

The Commission should adopt a more robust application process, especially if—despite TAPS's arguments—it adopts the case-by-case approach. As discussed in section II.A.2, the case-by-case approach requires that each application go through a fact-intensive, highly technical eligibility determination. If that approach is adopted, the Commission should establish a presumption that a protested case-by-case incentive application raises issues of material fact, and thus should be set for evidentiary hearing.[83]

A presumption that an evidentiary hearing is warranted will benefit consumers by providing discovery procedures and adequate time for a serious inquiry into whether the requested incentive satisfies the eligibility criteria and that the resulting rate is just and reasonable. That additional process is needed because much of the information that may be necessary to evaluate an application's potential security benefits is likely to be redacted as Critical Electric Infrastructure Information ("CEII"). The NOPR itself acknowledges that some information it receives related to advanced cybersecurity technology will include CEII and encourages a utility to seek protected treatment for any part of its filing seeking

---

[82] We note that Section 40124 of the Bipartisan Infrastructure Law, codified in 42 U.S.C. § 18723, authorizes a Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance program to support non-public utilities.

[83] Although the Commission's "choice . . . to hold an evidentiary hearing is generally discretionary," *Blumenthal v. FERC*, 613 F.3d 1142 (2010) (cleaned up), the Commission's practice is to establish hearing procedures when cases "raise[] issues of material fact that cannot be resolved based on the record before us and that are more appropriately addressed in the hearing and settlement judge procedures ordered below." *Union Elec. Co.*, 181 FERC 61,064, P 38 (2022); *see also Kan. Elec. Power Co.*, 181 FERC ¶ 61,017, PP 11-12 (2022) (affirming decision to establish hearing procedures to resolve disputed material facts); *Cf.* 18 C.F.R. § 385.217 (summary judgement appropriate only if "there is no genuine issue of fact material to the decision").

incentives that includes specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure.[84] In fact, a filing utility has incentive to overuse CEII designations—both to protect its security and to avoid ratepayer scrutiny—while the Commission's regulations provide no mechanism to discipline such overuse.

The Commission's usual filing procedures under Section 205 provide only twenty-one days from filing for a customer to file a protest. During that short time, a customer must: discover that an application has been made; submit an intervention and execute a protective agreement;[85] wait up to five business days for the applicant to provide the unredacted application;[86] analyze the complex, technical data; and prepare a protest or comments to submit to the Commission. And the Commission must act within sixty days to avoid the incentive going into effect as a matter of law. Given the resulting particularly heavy lift for customers protesting a cybersecurity incentive application, demonstrating a genuine issue of material fact will be difficult. A compressed timeline will prevent an incentive application from receiving the kind of meaningful Commission and customer evaluation necessary to ensure just and reasonable rates. The Commission should make clear that, should it adopt the case-by-case approach, all cybersecurity incentive applications will be presumed to raise issues of material fact, and will thus be subject to an evidentiary hearing with opportunity for discovery.[87] Such a presumption will help ensure (a) that any Commission decision on a case-by-case application will be based on substantial

---

[84] NOPR PP 16, 24 & n.23.

[85] 18 C.F.R. § 388.113(g)(4).

[86] *Id.* (if the applicant objects to disclosure, a customer could wait even longer than five business days).

[87] *Idaho Power Co.*, 117 FERC ¶ 63,050, P 12 (2006) ("[G]enuine issue[s] of material fact in dispute . . . must be adjudicated in a trial-type hearing.").

evidence, and (b) that the Commission's CEII regulations are properly used to limit dissemination of any CEII without allowing those same regulations to be used as a shield for utilities to avoid scrutiny of their incentive rates.

Even under the PQ List approach, the Commission should be liberal in setting matters for evidentiary hearings if requested by a customer to rebut the presumption. The PQ List approach is likely to reduce controversy, but if the proposed *rebuttable* presumption is to have any meaning, customers must have a sufficient opportunity to evaluate the application, seek discovery, and develop their case. In many such cases, evidentiary hearing procedures will likely be needed.

E. The Commission should explicitly exclude generators with market-based rates from incentive eligibility.

FPA section 219A encompasses incentives for wholesale energy sales.[88] The NOPR focuses on cost-of-service transmission rates,[89] but any entity with "a rate on file with the Commission" would be eligible for the incentive.[90] The NOPR does not discuss how, if at all, the incentives would be available to generators who sell at market-based rates. The Commission should expressly exclude wholesale energy sales at market-based rates from receiving this incentive.

Neither the ROE Incentive nor Regulatory Asset Incentive could reasonably be applied to market-based rate sales, which make up the vast majority of wholesale sales

---

[88] 16 U.S.C. § 824s-1(c) ("[T]he Commission shall establish, by rule, 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 public utilities . . . .") (emphasis added).

[89] *See, e.g.*, NOPR P 37 (referring to allocation of enterprise-wide investments to transmission); *id.* P 39 (referring to the regulatory asset being included "transmission rate base"); *id.* P 43.

[90] NOPR, Proposed Regulatory Text § 35.48. *See also, id.* P 34 & n. 31.

under the Commission's jurisdiction. Both incentives are implicitly premised on the applicant's filed rate being a cost-of-service rate, in which it is entitled to earn an ROE on its rate base.

Furthermore, even if some incentive mechanism were suggested in this rulemaking that could be applicable to entities that sell at market-based rates, the Commission should not adopt it in its final rule. The Commission has recognized the distorting effect of out-of-market payments.[91] Any financial incentive for a generator selling at market-based rates will have the potential to distort the competitive energy and ancillary services markets. Such a result would be unjust and unreasonable.

CONCLUSION

As discussed in these comments, any final rule in this proceeding must benefit consumers both by encouraging investment in technology that will enhance the security of public utilities *and* by ensuring that the resulting rates are just and reasonable.

---

[91] See, e.g., *Calpine Corp. v. PJM Interconnection L.L.C.*, 171 FERC ¶ 61,034 PP 26-27 (2018) (finding out-of-market payments distort wholesale capacity prices and compromise market integrity), *corrected*, 171 FERC ¶ 61,035 (2020); *id.* P 37 (recognizing "the well-established economic theory that out-of-market support distorts capacity market prices").

To satisfy both those requirements, the Commission should adopt TAPS's proposed modifications to the NOPR's proposal.

Respectfully submitted,

/s/ Cynthia S. Bogorad.

Cynthia S. Bogorad
Anree G. Little

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

November 7, 2022