UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

INITIAL COMMENTS OF THE EDISON ELECTRIC INSTITUTE

The Edison Electric Institute ("EEI") respectfully submits the following comments in response to the Federal Energy Regulatory Commission's ("FERC's" or "Commission's") Notice of Proposed Rulemaking ("NOPR") regarding the Commission's proposal, as directed by the Infrastructure Investment and Jobs Act of 2021 ("Infrastructure and Jobs Act"), to revise its regulations to provide incentive-based rate treatments to encourage investments by utilities in advanced cybersecurity technology and participation by utilities in cybersecurity threat information sharing programs.[1]

EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity for about 235 million Americans and operate in all 50 states and the District of Columbia. Collectively, the electric power industry supports more than seven million jobs in communities across the United States. EEI's members are committed to providing affordable and reliable electricity to customers now and in the future. EEI members own and operate jurisdictional transmission facilities in all regions of the country and, as such, are directly impacted by and can provide a broad-based perspective on the issues raised in the NOPR.

[1] *Incentives for Advances Cybersecurity Investment*, Notice of Proposed Rulemaking, 180 FERC ¶ 61,189 (Sept. 22, 2022) ("NOPR").

I. COMMISSION PROPOSAL

The Commission proposes a regulatory framework that outlines how a utility could qualify for incentives for eligible cybersecurity expenditures. Under this framework, the Commission proposes that eligible cybersecurity expenditures must: (1) materially improve cybersecurity either through an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program; and (2) not already be mandated by the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards, or local, state, or Federal law. The Commission proposes to evaluate cybersecurity investments using a list of pre-qualified expenditures ("PQ List") that are eligible for incentives, as determined by the Commission and publicly maintained on the Commission's website. Any cybersecurity expenditure that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive. The Commission also proposes an alternative approach, whereby a utility's cybersecurity expenditure would be evaluated on a case-by-case basis to determine if it is eligible for an incentive.

The Commission proposes two options for the type of incentive a utility could receive for an eligible cybersecurity expenditure: (1) a return on equity ("ROE") adder of up to 200 basis points, or (2) deferred cost recovery for certain cybersecurity expenditures that enables the utility to defer expenses and include the unamortized portion in rate base. Any approved incentive would remain in effect for five years from the date on which the cybersecurity investment enters service or expenses are incurred, but would expire earlier if other conditions are met before the end of that five-year period. Approved cybersecurity incentives would be subject to an annual informational filing.

II. COMMENTS

A. EEI Member Companies Generally Support the Commission's Proposal to Allow Incentive-Based Rate Treatments

The Commission proposes to provide a process for utilities to qualify for and receive incentive-based rate treatments for eligible cybersecurity expenditures. Consistent with EEI members' responsibility to provide safe, reliable, increasingly clean energy, protecting the energy infrastructure from cybersecurity threats is a top priority for the nation's electric companies. Knowing that sophisticated adversaries seek to identify potentially exploitable vulnerabilities with the intent to attack the electric grid, EEI members continually look for additional measures that enhance the electric power sector's efforts to address grid-related threats while balancing the many demands utilities face for prioritizing limited capital. Although there are many demands for limited capital, electric utilities make regular investments in cybersecurity protection inclusive higher priority assets. These investments to help safeguard the energy grid and are made despite the fact that companies do not earn a return on all of the operating and maintenance ("O&M") costs needed to implement cybersecurity programs. In some cases, these O&M costs are relatively high when compared to the capital costs of a cybersecurity program.

EEI appreciates the Commission's recognition of the need for greater cybersecurity protections in light of evolving and ever-present threats and the role that incentives can play to elevate the level of cybersecurity and preparedness, commensurate with company-specific needs and risks. The energy sector faces numerous and complex cybersecurity challenges. These growing threats come at a time of both great change in the operation of the transmission system and an increase in the number and nature of attack methods. EEI generally supports the proposal in the NOPR to allow utilities to seek incentive-based rate treatments. There is both cost and benefit associated with going above and beyond what is required by the CIP Reliability

Standards, and the Commission's incentive proposal, with some modification, has the potential to balance those interests.

B. The Commission Should Adopt Both Proposed Approaches for Evaluating Cybersecurity Expenditure Eligibility

The Commission proposes two alternative approaches for evaluate ng expenditures: (1) the PQ List for cybersecurity expenditures, or (2) a case-by-case approach. As discussed below, the Commission should not limit the approach to either the PQ List or the case-by-case approach; both should be available avenues for utilities to pursue incentives for cybersecurity expenditures.

The Commission proposes that a utility seeking an incentive would be required to demonstrate that its cybersecurity expenditure qualifies as one or more of the PQ List items and is therefore entitled to a rebuttable presumption of eligibility for an incentive. EEI supports the Commission's proposal to use a PQ List and agrees with the Commission that utility-specific incentive filings could be substantially streamlined. Providing a PQ List will afford some level of assurance to utilities that an expenditure will qualify for incentives, which in turn may facilitate capital planning, reduce regulatory burden and accelerate the project.

The Commission should also adopt the case-by-case approach whereby a utility may file for incentive-based rate treatment for any cybersecurity expenditure that satisfies the eligibility criteria. Such a case-by-case approach should be in addition to, not in lieu of the PQ List approach. Because the PQ List approach would limit expenditures eligible for incentives only to those on the PQ List and would require the Commission to review and update the PQ List on a regular basis, especially in light of the rapid technology changes in this area. Limiting the approach to only the PQ List could delay the eligibility of cybersecurity expenditures for incentives until the list is updated. The case-by-case approach will allow flexibility for utilities

who have innovative methods for approaching cybersecurity that otherwise would take time through the rulemaking process to be added to the PQ List.

1. Initial PQ List

The Commission proposes to include two eligible cybersecurity expenditures on the PQ List initially: (1) expenditures associated with participation in CRISP; and (2) expenditures associated with internal network security monitoring within the utility's cyber systems, which could include information technology cyber systems and/or operational technology cyber systems, and which could be associated with cyber systems that may or may not be subject to the CIP Reliability Standards. The Commission initially proposes to include CRISP, as its purpose is to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the energy sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.

As noted above, both the use of a list of prequalified investments eligible for incentives and the initial list offered by the Commission are reasonable. If the Commission does not allow use of both, the Commission should supplement the list in the Final Rule to allow utilities more flexibility to determine the best controls and method of implementation in their environments.

As to the specific investments the Commission proposes to include on the initial PQ List, internal network security monitoring should be included, but the Commission should extend the expenditure eligibility to a broader set of cybersecurity capabilities across protective and detective controls not limited to those specific to network security monitoring. As the Commission notes, while the currently effective CIP Reliability Standards do not require internal network security monitoring, NERC has recognized the proliferation and usefulness of such technology. Other investments that should be added to the PQ List are: investments that deliver

capability across the Identify, Protect and Detect functions as defined by NIST; technology and processes including consulting services designed to incrementally implement principles of zero trust architecture; technology and processes to develop active threat hunting capability within IT and OT environments including, incident response retainer fees, penetration tests or vulnerability assessments; technology and processes to implement, manage, and monitor secure coding practices to include consulting services to navigate Software Bill of Materials requirements and leading practices; technology and processes to implement, manage, and monitor data loss prevention capability, including both IT- and OT-related sensitive data; and technology and processes to implement, manage, and monitor user and endpoint behavioral analysis.

With regard to the Commission's request for comment on whether to include other information sharing programs on the PQ List, EEI suggests that the Commission expand the list to include other federally funded or supported information sharing programs.

2. Updating the PQ List

The Commission states that it expects to regularly evaluate the PQ List and update it as necessary. 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.[2] The Commission would update the PQ List by adding, removing, or modifying cybersecurity expenditures, as needed, via a rulemaking, whether *sua sponte* or in response to a petition. EEI agrees that the list should be updated and, given the rapidly evolving cybersecurity landscape, updates should be implemented on a regular basis and include any items approved via the case-by-case process. EEI suggests

[2] If a particular cybersecurity expenditure becomes mandatory with respect to a utility, the provisions of proposed 18 CFR 35.48(f) would prohibit that utility from continuing to receive an incentive for the affected cybersecurity expenditure even if the Commission has not yet updated the PQ List.

that the Commission commit to a regular cadence to determine whether the list should be updated, e.g., no less than annually. This will allow the Commission to incorporate findings from any case-by-case showings. EEI also requests that the Commission revise the effective date on which the incentive would no longer be eligible to coincide with the date the Commission updates the PQ List as opposed to the effective date of any mandate.

C. Both Eligibility Criteria Are Appropriate for Incentivizing Cybersecurity Investment

To be eligible for incentive-based rate treatment, the Commission proposes that the utility seeking such treatment must demonstrate, at a minimum, that the expenditure: (1) would "materially improve" cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program(s); and (2) is not already mandated by CIP Reliability Standards, or otherwise mandated by local, state, or Federal law. The Commission states that, in determining which cybersecurity expenditures will materially improve a utility's security posture, it will consider six sources: (1) security controls enumerated in the NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations" catalog; (2) security controls satisfying an objective found in the NIST Cybersecurity Framework; (3) a specific recommendation from the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") or from the Department of Energy ("DOE"); (4) a specific recommendation from the CISA Shields Up Campaign; (5) participation in the DOE Cybersecurity Risk Information Sharing Program ("CRISP") or similar information sharing program; and/or (6) the Cybersecurity Capability Maturity Model ("C2M2") Domains at the highest Maturity Indicator Level ("MIL").

EEI supports the Commission's proposal to recognize either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program

via incentive rate treatment. As a general matter, utilities should be permitted to demonstrate that a specific investment warrants the requested incentive. The six sources the Commission proposes to consider when considering an incentive support this approach and are appropriate because these programs and agencies allow utilities flexibility to seek incentives for investments tailored to their individual risks and system design, as well as inherently recognize the evolving nature of cybersecurity risks. That said, utilities should be able to propose other sources beside the six listed by the Commission. EEI also supports the Commission's proposal to limit the opportunity for cybersecurity incentives to those investments not mandated by NERC or the federal, state, or local governments.

However, the Commission should discard the term "materially improve," which is not in the statutory language, nor defined in the NOPR, and should instead consider the fundamental program capabilities that provide the greatest coverage, protection, and resilience for the respective cybersecurity investment. The Commission explains that using the six sources from other agencies will help it to ensure that the cyber expenditures are targeted and effective. Given this, it is not clear what additional insights the Commission will glean from the application of a "materially improve" test, which will amount to a subjective exercise that may be difficult for the Commission to apply consistently.

Moreover, subjecting cyber investments to a materiality test for using any of the above six sources may not necessarily advance cybersecurity posture of electric companies, which should be the Commission's goal. For example, while C2M2 may be useful, restricting incentive eligibility to only those at the highest MIL may lead to overinvestment in unnecessary controls. Not all controls need to be the highest MIL to be both targeted and effective. This is especially true if a utility achieves an incrementally lower MIL and then C2M2 is updated to

include a higher MIL level. Such an action would not diminish the risk reduction value of these controls, but would needlessly render them ineligible for incentives, based on the Commission's proposed approach.

A better approach would be to enable the utility to provide the context for why a security-related investment promotes a targeted level of cyber maturity. This would avoid the unintended consequence of overinvestment in unnecessary or extraneous controls, while at the same time providing an opportunity to encourage investment in controls that a company has determined to provide the greatest benefit relative to a comprehensive risk-based assessment of the proprietary protections and controls positioned to protect an organization's most critical assets. The Commission should allow a utility to describe how the investment achieves the outcomes of enhanced cybersecurity capabilities through a modern cybersecurity risk management and control framework and not default to what could be overly simplistic proxies in a manner that could have unintended consequences.

D. EEI Supports the Two Rate Incentives

The Commission proposes the following rate incentives for utilities that make eligible cybersecurity investments: (1) an ROE adder of 200 basis points that would be applied to the incentive-eligible investments; and (2) deferral of certain eligible expenses for rate recovery, enabling them to be part of rate base such that a return can be earned on the unamortized portion.

EEI supports the NOPR's proposal to provide ROE incentives to utilities for cybersecurity investments. Specifically, EEI supports the proposal to authorize utilities an ROE adder of up to 200 basis points for eligible cybersecurity investments. Some cybersecurity investments involve relatively low dollar amounts, compared with other capital investments, in addition to the fact that these investments are recovered over a short period of time, the proposed

200 basis point adder is reasonable has the potential to create an incentive that will shift utility cybersecurity expenditures in the manner intended by the Commission and Congress.

EEI supports the Commission's proposal to allow enterprise-wide investments and not just certain investments. The Commission's enterprise-wide approach avoids the potential for investments to be funneled to only certain assets, leaving other areas (e.g., network assets, generation) potentially ineligible and aligns with Commission policies on enabling access for and deployment of distributed energy resources and advanced technologies.[3]

As noted, the Commission also proposes to allow a utility that makes eligible cybersecurity investments to seek deferred cost recovery. Specifically, the Commission proposes that expenses that would otherwise be eligible for inclusion in cost-of-service rates as current period expenses may receive an incentive by deferring such costs as regulatory assets if they are incurred after the effective date of the Commission order granting a utility's request for incentives. Consistent with the proposal for the ROE incentive for eligible cybersecurity capital investments, the Commission proposes that only directly assigned transmission costs or the conventionally allocated portion of enterprise-wide expenses (e.g., using the wages and salaries allocator) would be eligible for the regulatory asset incentive in transmission rates.

The Commission explains that it may be appropriate to allow a utility to defer recovery of certain cybersecurity costs that are generally expensed as they are incurred (e.g., third-party provision of hardware, software, and computing and networking services; recurring subscription costs and implementation costs such as training to implement new cybersecurity practices that is distinct from costs associated with pre-existing training on cybersecurity practices; dues for participation in threat information sharing programs; internal system evaluations and assessments

[3] EEI seeks clarification that an allocable share of costs may be recovered through not only transmission rates but also other cost-based rates.

or analyses by third parties) and treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base. The Commission preliminarily has found that costs that are allowed to be deferred as a regulatory asset should be included in rate base for determination of the base return but not for the additional return associated with the 200 basis point ROE adder, i.e., an investment cannot receive both a basis point ROE and regulatory asset treatment.

Finally, because FPA section 219A(c)(2) directs the Commission to offer incentives to encourage *participation* by public utilities in cybersecurity threat information sharing programs, the Commission seeks comment on utilities that are already participating in an eligible cybersecurity threat information sharing program should be eligible to seek to recover this incentive.

The Commission should allow the regulatory asset treatment for ongoing participation including by those that are already participating in such programs. Participation in these programs is not a static event; it is ongoing and continued participation should be encouraged. CRISP participants have to refresh the technology from time to time, which is a new, potentially capital expenditure, as well as the annual costs to stay in the program as a participant.

EEI suggests that the Commission include training, implementation, software costs, and allow cloud computing expenses to also be allowed to be deferred as a regulatory asset.

EEI is concerned with the proposal to limit the eligible costs to those associated with implementing cybersecurity upgrades and to not include ongoing costs including system maintenance, surveillance, and other labor costs, either in the form of employee salaries or third-party service contracts. Including these costs would support the Commission's cybersecurity goals, incent best practices, and benefit customers by reducing the possibility of interruptions

from cyber-attacks. The Commission should confirm that eligible expenses for the regulatory asset incentive include costs that are charged to O&M and/or A&G accounts so that costs such as the above are includable.

E. Performance-Based Rates

Section 219A(c) of the FPA directs the Commission to establish incentive-based, including performance-based, rate treatments. In the NOPR, the Commission seeks comment on performance-based rates and whether and how the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.[4] The Commission seeks comment on specific cybersecurity metrics that could be subject to a performance standard, and specifically whether any widely accepted metrics for cybersecurity performance could lend themselves to be benchmarks needed for performance-based rates, or whether new appropriate metrics could be developed. It also seeks comment on the rate mechanisms that could accompany such metrics. The Commission states that any proposed mechanisms should: (1) rely on cybersecurity performance benchmarks and not expenditures or practices; and (2) consider ratepayer impacts, given the relatively small costs of cybersecurity expenditures compared to utilities' overall cost-of-service.

Without clear, industry-wide metrics, a performance-based program would be difficult to implement. In addition, given the considerable work ahead on cybersecurity maturity, the notion of performance-based ratemaking may be premature not to mention challenging to develop and

[4] Consistent with Order No. 679, which implemented FPA section 219, we interpret "incentive-based, including performance-based, rate treatments" in FPA section 219A to require the Commission to consider performance-based rates as an option among incentive ratemaking treatments. *Promoting Transmission Inv. through Pricing Reform*, Order No. 679, 71 FR 43293 (July 31, 2006), 116 FERC ¶ 61,057 (2006), *order on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *order on reh'g*, 119 FERC ¶ 61,062 (2007).

implement successfully. Moreover, the notion of performance or success is difficult, because even with best preparations, a company could still have an attack given that attacks are nearly constant. A successful attack may not be a reflection on whether the incentives did what Congress intended.

F. Cybersecurity ROE Incentive Duration

The Commission proposes to allow a utility granted a ROE incentive to receive that incentive until the earliest of: (1) the conclusion of the depreciation life of the underlying asset; (2) five years from when the cybersecurity investment(s) enter service;[5] (3) the time that the investment(s) or activities that serve as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission, or local, state, or Federal law; or (4) the recipient no longer meets the requirements for receiving the incentive. The Commission explains that incentive-eligible cybersecurity investments primarily include equipment or system modifications that typically have short depreciation lives, as opposed to long-lived assets like physical structures, and thus most cybersecurity incentives granted under this rulemaking would remain in effect until the conclusion of the depreciation life of the underlying asset. However, for investments with useful lives exceeding five years, the Commission proposes that the incentive end at the conclusion of five years from the time that the asset receiving the cybersecurity incentive entered service.

The five-year period may be reasonable, but if the utility has a cybersecurity asset with a longer depreciation life, the utility should have the option to make an argument for a longer incentives period, depending on the investment on a case-by-case basis.

[5] For participation in an information sharing program, the "investment" would recur annually.

In addition, if an incentive becomes mandatory it is not clear why it must end automatically. For example, why, if the investment is in year three and then in year four it becomes a mandatory standard, a utility should lose the incentive going forward. The Commission's proposed approach will dampen potential incentives to do the work to be an early adopter of promising, qualifying cybersecurity measures.

G. Regulatory Asset Incentive Duration and Amortization Period

The Commission proposes that a utility granted the regulatory asset incentive must amortize the regulatory asset over five years, and that a utility granted the incentive may defer eligible expenses for up to five years from the date of Commission approval of the incentive. Under this provision, eligible expenses incurred for five years could be added to the regulatory asset that is allowed in rate base and amortized over five subsequent years. EEI requests clarification that the amortization period would be up to five years, but that five years is not the only duration for amortization.

The Commission proposes to make an exception to this sunsetting provision for eligible cybersecurity threat information sharing programs on the basis that they are distinct from discrete cybersecurity investments that may become obsolete with the passage of time. FPA section 219A(c)(2) directs the Commission to provide incentives for participation in cybersecurity threat information sharing programs. Thus, the Commission proposes that utilities be able to continue deferring these expenses and including them in their rate base for each annual tranche of expenses, for as long as: (1) the utility continues incurring costs for its participation in the program, and (2) the program remains eligible for incentives. EEI supports the Commission proposals and underscores the value of information sharing about the nature of threats which help electric utilities react to and mitigate the threat.

H. Reporting Requirements

The Commission proposes regulations to require utilities to submit informational reports to the Commission for the duration of any awarded incentive. A utility that has received cybersecurity incentives under this section must make an annual informational filing by June 1, provided that the utility has received Commission approval for the incentive at least 60 days prior to June 1 of that year. Utilities that receive Commission approval for an incentive later than 60 days prior to June 1 would be required to submit an annual informational filing beginning on June 1 of the following year.[6] The annual filing should detail the specific investments, if any, as of that date, that were made pursuant to the Commission's approval and the corresponding FERC account for which expenditures are booked. For recipients of the ROE incentive, each annual informational filing should describe the parts of its network that it upgraded in addition to the nature and cost of the various investments. For recipients of the regulatory asset incentive, each annual informational filing should describe such expenses in sufficient detail to demonstrate that such expenses are specifically related to the eligible cybersecurity investment underlying the incentives and not for ongoing services including system maintenance, surveillance, and other labor costs. The Commission also states it may also conduct periodic verification to assess cybersecurity investments and expenses for which it has approved incentives. The Commission could perform such verifications through multiple means and should balance the manner in which verifications are conducted (i.e., directing further informational filings, oral briefings) with the administrative burden of providing and protecting the information. For example, while the annual informational filings will inform the

[6] If a utility first receives Commission-approval for the incentive on April 1 or later, the initial annual informational filing would be due on June 1 of the following year.

Commission on how and when any additional verification is warranted, they reveal proprietary/confidential information relative to a security program whereas oral briefings may mitigate some of the concern around both audits and informational filings.

As a utility's cybersecurity protections contain some of the most sensitive information for utilities, there would be a need for applicants to limit disclosure of the information in an annual report. While EEI recognizes that the Commission needs information on which to make a determination, disclosure of this information could create a security risk which runs counter to the Commission's goals in this proceeding. The Commission appropriately recognizes the importance of balancing confidentiality with the needs for transparency in determining the initial incentive and that such considerations are balanced through Critical Energy/Electric Infrastructure Information ("CEII") filings noting that "a utility should seek CEII treatment, as appropriate, for any part of its filing seeking incentives that includes specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure."[7] Just as it allows applicants to seek CEII treatment for the rate incentive filings, the Commission should also allow the annual reports to be filed under the CEII regulations because the information the Commission seeks, while innocuous on its own, could be coupled with other information and used by those seeking to attack the reliability of U.S. energy infrastructure. To be clear, EEI does not oppose the reporting requirement generally, but the NOPR proposes to include information about types of upgrades and the nature and cost of various investments. Disclosure of this information creates security concerns, and the Commission should permit utilities to seek CEII treatment for these filings. Given the sensitivity of information filed as part of an annual report, electric companies would need assurances regarding how the various

[7] NOPR at P 24.

intervenor/third-party recipients of CEII would comply with sensitive data and information protection requirements, the obligation to destroy CEII when requested to do so, the prohibition on sharing CEII, and immediate reporting of unauthorized access of CEII.

III. CONCLUSION

EEI generally supports the proposal in the NOPR to allow utilities to seek incentive-based rate treatments and the Commission's incentive proposal, with the modifications and clarifications described above, has the potential to balance those interests.

Respectfully submitted,

/s/

Bob Stroh
Associate General Counsel, Reliability and Security
(202) 508-5145
rstroh@eei.org

Edison Electric Institute
701 Pennsylvania Ave., N.W.
Washington, DC 20004

November 7, 2022