This document is scheduled to be published in the
Federal Register on 10/06/2022 and available online at
federalregister.gov/d/2022-21003, and on **govinfo.gov**

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 35

[Docket Nos. RM22-19-000; RM21-3-000]

Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking; notice terminating proceeding.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to revise its regulations to provide incentive-based rate treatments for the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by utilities for the purpose of benefitting consumers by encouraging investments by utilities in advanced cybersecurity technology and participation by utilities in cybersecurity threat information sharing programs, as directed by the Infrastructure Investment and Jobs Act of 2021 (Infrastructure and Jobs Act). This notice of proposed rulemaking (NOPR) also terminates the NOPR proceeding in Docket No. RM21-3-000 (December 2020 Cybersecurity Incentives NOPR).

DATES: As of [**INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, the proposed rule published at 86 FR 8309 on February 5, 2021, is withdrawn. Comments on this proposed rule are due **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways. Electronic filing through https://www.ferc.gov, is preferred.

- Electronic Filing: Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format.
- For those unable to file electronically, comments may be filed by USPS mail or by hand (including courier) delivery.
    - Mail via U.S. Postal Service Only: Addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, DC 20426.
    - Hand (including courier) delivery: Deliver to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

The Comment Procedures Section of this document contains more detailed filing procedures.

FOR FURTHER INFORMATION CONTACT:

Kal Ayoub (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

(202) 502-8863
kal.ayoub@ferc.gov

David DeFalaise (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8180
david.defalaise@ferc.gov

Adam Pollock (Technical Information)
Office of Energy Market Regulation
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8458
adam.pollock@ferc.gov

Alan Rukin (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8502
alan.rukin@ferc.gov

SUPPLEMENTARY INFORMATION:

TABLE OF CONTENTS

I. Introduction

1. In this NOPR, the Commission proposes under section 219A of the Federal Power Act (FPA)[1] to establish rules for incentive-based rate treatments for certain voluntary cybersecurity investments[2] by utilities.[3] These rules would make incentives available to utilities that make certain cybersecurity expenditures that enhance their security posture by improving their ability to protect against, detect, respond to, or recover from a cybersecurity threat and to utilities that participate in cybersecurity threat information sharing programs to the benefit of ratepayers and national security.

2. First, we propose a regulatory framework on how a utility could qualify for incentives for eligible cybersecurity expenditures. Under this framework, we propose that eligible cybersecurity expenditures must: (1) materially improve cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program; and (2) not

---

[1] Infrastructure and Jobs Act, Pub. L. 117-58, section 40123, 135 Stat. 429, 951 (to be codified at 16 U.S.C. 824s-1).

[2] In this NOPR, the term "investments" in cybersecurity technology means expenditures that can be either capitalized costs or expenses.

[3] Notwithstanding that Infrastructure and Jobs Act requires the Commission to offer incentives to "public utilities," we propose to make rate incentives available to non-public utilities that have or will have a rate on file with the Commission, similar to Commission precedent under FPA section 219, 16 U.S.C. 824s. Therefore, all references in this NOPR to "utilities" are intended to include both public utilities and non-public utilities that have or will have a rate on file with the Commission.

already be mandated by Critical Infrastructure Protection (CIP) Reliability Standards, or local, state, or Federal law. A utility would seek an incentive in a filing pursuant to FPA section 205[4] and the incentive would be effective no earlier than the date of the Commission order approving the incentive request.

3. We propose to evaluate cybersecurity investments using a list of pre-qualified expenditures that are eligible for incentives determined by the Commission and publicly maintained on the Commission's website (PQ List). With the Commission having evaluated expenditures to include on the PQ List in advance, we believe that the PQ List approach would provide an efficient and transparent mechanism for determining appropriate cybersecurity expenditures that are eligible for incentives. We propose that any cybersecurity expenditure that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive. We also discuss and seek comment on a potential 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.

4. Second, we propose two options for the type of incentive a utility could receive for an eligible cybersecurity expenditure: (1) a return on equity (ROE) adder of 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.

---

[4] 16 U.S.C. 824d.

5. Third, we propose that any approved incentive(s) will remain in effect for five years from the date on which the cybersecurity investment(s) enters service or expenses are incurred, or expire earlier if other conditions discussed in this NOPR are met before the end of that five year period. We seek comment on the proposed duration and expiration conditions for incentives granted under this proposal.

6. Finally, we propose that a utility that has received a cybersecurity incentive under this section must make an annual informational filing on June 1, as further discussed herein. The annual filing should detail the specific investments that were made pursuant to the Commission's approval and the corresponding FERC account used.[5]

II. <u>Background</u>

A. <u>Infrastructure Investment and Jobs Act of 2021</u>

7. On November 15, 2021, the Infrastructure and Jobs Act was signed into law.[6] The Infrastructure and Jobs Act, in part, directs the Commission to revise its regulations to 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 for the purpose of benefitting consumers by encouraging investments by public

---

[5] *See* 18 CFR part 141.

[6] Infrastructure and Jobs Act, Pub. L. 117-58, 135 Stat. 429.

utilities in advanced cybersecurity technology[7] and participation by public utilities in cybersecurity threat information sharing programs.

8. As an initial step in the process of revising the Commission's regulations, the Infrastructure and Jobs Act directed the Commission to conduct a study, in consultation with certain entities,[8] to identify incentive-based rate treatments, including performance-based rates, for the jurisdictional transmission and sale of electric energy that could support investments in advanced cybersecurity technology and participation by public utilities in cybersecurity threat information sharing programs.[9] The Infrastructure and Jobs Act also required the Commission to submit a report to Congress (Report) detailing the results of the directed study. Following the passage of the Infrastructure and Jobs Act, Commission staff

---

[7] FPA section 219A(a)(1) defines the term advanced cybersecurity technology to mean any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances the security posture of public utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat. Infrastructure and Jobs Act, Pub. L. 117-58, section 40123, 135 Stat. 429, 951 (to be codified at 16 U.S.C. 824s-1(a)(1)). FPA section 219A(a)(2) defines the term advanced cybersecurity technology information to mean information relating to advanced cybersecurity technology or proposed advanced cybersecurity technology that is generated by or provided to the Commission or another Federal agency. *Id.* at 952 (to be codified at 16 U.S.C. 824s-1(a)(2)).

[8] The entities identified in the Infrastructure and Jobs Act are: Secretary of Energy; North American Electric Reliability Corporation (NERC); Electricity Subsector Coordinating Council (ESCC); and National Association of Regulatory Utility Commissioners (NARUC).

[9] Infrastructure and Jobs Act, Pub. L. 117-58, section 40123, 135 Stat. 429, 952 (to be codified at 16 U.S.C. 824s-1(b)).

consulted with the specified entities to help identify incentive-based rate treatments that could enhance the security posture of the Bulk-Power System.[10]

9. On May 13, 2022, the Report was submitted to Congress.[11] The Report, among other things, outlined prior Commission efforts to address incentives for cybersecurity initiatives. The Report provided information regarding potential incentive-based rate treatments and the Commission's general ratemaking authority, including the prior adoption of rate incentives and performance-based ratemaking in other contexts. In addition, the Report discussed challenges associated with adopting an incentive-based rate structure to enhance the security posture of the Bulk-Power System. The Report noted that, while advanced technologies that address cybersecurity threats may be innovative and/or above and beyond industry standards at one time, they may subsequently become conventional, mandatory, or even antiquated and therefore may be less deserving of an incentive over time.

---

[10] The term Bulk-Power System is defined in FPA section 215 and refers to: (1) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (2) electric energy from generation facilities needed to maintain transmission system reliability. 16 U.S.C. 824o(a)(1). With respect to CIP Reliability Standards, NERC uses the term "bulk electric system" (BES), which is generally defined as transmission facilities that are operated at 100 kV or higher and real power or reactive power resources connected at 100 kV or higher. *See* NERC, Glossary of Terms Used in NERC Reliability Standards (March 29, 2022), https://www.nerc.com/files/glossary_of_terms.pdf.

[11] FERC, *Incentives for Advanced Cybersecurity Technology Investment* (May 2022).

B. Prior Commission Action on Cybersecurity Incentives

10. The Commission began assessing the potential use of incentives to improve cybersecurity prior to the passage of the Infrastructure and Jobs Act. On June 18, 2020, Commission staff issued a white paper to explore a potential framework for providing transmission incentives to utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the mandatory and enforceable CIP Reliability Standards.[12] Following the issuance of the Cybersecurity White Paper, the Commission issued the December 2020 Cybersecurity Incentives NOPR on December 17, 2020, proposing to allow utilities to request incentives for certain cybersecurity investments that go above and beyond the requirements of the CIP Reliability Standards.[13]

11. In the December 2020 Cybersecurity Incentives NOPR, the Commission proposed two cybersecurity incentive approaches. The first approach, referred to as the NERC CIP Incentives Approach, would have allowed an entity to receive incentive-based rate treatment for voluntarily applying identified CIP Reliability Standards to facilities that were not otherwise subject to those requirements. The

---

[12] FERC, *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19-000, (June 2020) (Cybersecurity White Paper), https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf.

[13] *Cybersecurity Incentives*, Notice of Proposed Rulemaking, 86 FR 8309 (Feb. 5, 2021), 173 FERC ¶ 61,240 (2020).

second approach, the National Institute of Standards and Technology (NIST) Framework Approach, would have allowed an entity to receive incentive-based rate treatment for implementing certain security controls included in the NIST Framework[14] that exceed the requirements of the CIP Reliability Standards.

12. In light of the Congressional mandate in the Infrastructure and Jobs Act directing the Commission to establish cybersecurity incentives, this NOPR supersedes the December 2020 Cybersecurity Incentives NOPR, and that proceeding in Docket No. RM21-3-000 is hereby terminated.

C. Advanced Cybersecurity Technology and Information

1. Advanced Cybersecurity Technology

13. As noted above, the Infrastructure and Jobs Act directs the Commission to, among other things, identify incentive-based rate treatments that could support investments in advanced cybersecurity technology. An advanced cybersecurity technology can be a product and/or a service.[15]

---

[14] NIST is a part of the U.S. Department of Commerce that advances measurement science, standards, and technology. It has developed a voluntary Framework for Improving Critical Infrastructure Cybersecurity to "address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses." NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[15] *See supra* n.7 (defining advanced cybersecurity technology).

14. Cybersecurity products are generally hardware, software, and cybersecurity services that can be used for information technology systems and/or operational technology[16] systems. Cybersecurity products can include, but are not limited to, security information and event management systems, intrusion detection systems, anomaly detection systems, encryption tools, data loss prevention systems, forensic toolkits, incident response tools, imaging tools, network behavior analysis tools, access management systems, configuration management systems, anti-malware tools, user behavior analytic software, event logging systems, and any system for access control, identification, authentication, and/or authorization control.

15. Cybersecurity services may be either automated or manual and can include, but are not limited to, system installation and maintenance, network administration, asset management, threat and vulnerability management, training, incident response, forensic investigation, network monitoring, data sharing, data recovery, disaster recovery, network restoration, log analytics, cloud network storage, and any general cybersecurity consulting service.

---

[16] The NIST glossary defines "operational technology" as "programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms." NIST, Computer Security Resource Center, Glossary (Mar. 10, 2022), https://csrc.nist.gov/glossary.

2. Advanced Cybersecurity Technology Information

16. Advanced cybersecurity technology information may include, but is not limited to, plans, policies, procedures, specifications, implementation, configuration, manuals, instructions, accounting, financials, logs, records, and physical or electronic access lists related to or regarding the advanced cybersecurity technology. Some advanced cybersecurity technology information that is provided to the Commission may constitute critical energy/electric infrastructure information (CEII).[17]

D. Cybersecurity Threat Information Sharing Programs

17. The Infrastructure and Jobs Act also directs the Commission to identify incentive-based rate treatments that could support participation by public utilities in cybersecurity threat information sharing programs. Engagement with the entities as directed in the Infrastructure and Jobs Act informed the Commission of the existing barriers faced by utilities seeking to participate in these information sharing programs, which include the high costs associated with implementing monitoring technology and maintenance of sensor technology, the amount of time and effort required to share information, incurring fees to participate in information sharing programs, and concerns regarding the confidentiality of the information once shared.

---

[17] 18 CFR 388.113.

III. Discussion

18. To implement the statutory directive in the Infrastructure and Jobs Act, we propose to revise our regulations to provide a process for utilities to qualify for and then receive incentive-based rate treatments for eligible cybersecurity expenditures. For purposes of this NOPR, an "expenditure" includes both expenses and capitalized costs associated with advanced cybersecurity technology and participation in a cybersecurity threat information sharing program. We propose the following approach and then seek comments on our proposal in three sections: (1) Proposed Approaches to Request an Incentive, which discusses how a utility could qualify for incentives for eligible cybersecurity expenditures; (2) Proposed Rate Incentives, which describes the type of incentive a utility could receive for an eligible cybersecurity expenditure; and (3) Proposed Incentive Implementation, which discusses proposed duration and expiration conditions for incentives.

A. Proposed Approaches to Request an Incentive

19. We propose to add § 35.48(c) to our regulations to create a framework for evaluating whether certain cybersecurity expenditures, including expenses and capitalized costs, qualify for an incentive. First, we propose eligibility criteria to determine whether a cybersecurity expenditure is eligible for an incentive. Second, in § 35.48(d) we propose to use a list of pre-qualified investments, the PQ List, to identify the types of cybersecurity expenditures that the Commission will find eligible for an incentive. In addition, we seek comment on whether a

case-by-case approach should be used to evaluate whether certain cybersecurity expenditures are eligible for incentives.

1. **<u>Eligibility Criteria</u>**

20. We propose that the utility seeking an incentive 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. With respect to the first criterion, we seek comment on whether, and if so how, the Commission should evaluate and ensure that the benefits of the expenditure exceed the combined costs of the expenditure and incentive, to ensure the proposed rates are just and reasonable. Further, we seek comment on whether these are the appropriate criteria and whether there are additional criteria or limitations that we should consider (e.g., whether the Commission should consider an obligation imposed by a state commission as a condition for a merger to be ineligible for an incentive).

21. Additionally, we propose that, in determining which cybersecurity expenditures will materially improve a utility's security posture, the Commission will consider the following sources: (1) security controls enumerated in the NIST SP 800-53 "Security and Privacy Controls for Information Systems and

Organizations" catalog;[18] (2) security controls satisfying an objective found in the NIST Cybersecurity Framework;[19] (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);[20] (4) a specific recommendation from the CISA Shields Up Campaign;[21] (5) participation in the DOE Cybersecurity Risk information Sharing Program (CRISP) or similar information sharing program; and/or (6) the Cybersecurity Capability Maturity Model Domains at the highest Maturity Indicator Level.[22] Using vehicles from DHS, DOE, and other agencies responsible for addressing sophisticated and rapidly evolving cyber threats as qualifiers for the consideration of incentives would allow the Commission to benefit from the expertise of other federal agencies and help ensure that the cybersecurity expenditures will be targeted and effective.

---

[18] NIST, Special Publication 800-53, Revision 5*, Security and Privacy Controls for Information Systems and Organizations*, (Dec. 12, 2020), https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.

[19] *See* NIST, *Cybersecurity Framework*, https://www.nist.gov/cyberframework.

[20] S*ee*, e.g., CISA, *National Cyber Awareness System Alerts*, https://www.cisa.gov/uscert/ncas/alerts.

[21] *See* CISA, *Shields Up*, https://www.cisa.gov/shields-up.

[22] *See* DOE, *Cybersecurity Capability Maturity Model*, https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

22. We propose that, to be eligible for incentive-based rate treatment, cybersecurity expenditures must satisfy the first two criteria (i.e., materially improve cybersecurity and not already mandated). The eligibility criteria would apply to either of the two evaluation approaches discussed below (i.e., the PQ List or the case-by-case approach). We seek comment on these criteria, including any potential refinements, and any other criteria for incentive eligibility that the Commission should adopt in the Final Rule.

2. **Proposed Approaches for Evaluating Cybersecurity Expenditure Eligibility**

23. We propose adopting a PQ List approach, which would use a list of pre-qualified cybersecurity expenditures, consistent with the eligibility criteria that the Commission ultimately adopts. We also seek comment on the alternative use of a case-by-case approach.

24. Under either approach, we propose that a utility make a filing pursuant to FPA section 205 for incentive-based rate treatment for those expenditures. Consistent with our precedent for incentives under FPA section 219, while a utility may first file a petition for declaratory order to seek a ruling on its eligibility for an incentive, a utility still must make a filing under FPA section 205 for Commission review of any rate changes. We propose that the incentive would be effective no earlier than the date of the Commission order granting the incentive under FPA section 205. 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.[23]

a. <u>PQ List Approach</u>

25. We propose to create a PQ List that identifies expenditures that could warrant an incentive. Under this proposal, the PQ List will be codified at 35.48(d) of the Commission's regulations and a copy will be posted on the Commission's website.

26. We propose 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. Any cybersecurity expenditure that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive. Although the PQ List items would be entitled to a presumption of eligibility, the utility would still need to demonstrate, and the Commission would need to find, that the proposed rate, inclusive of the incentive, is just and reasonable. We propose to allow intervening parties to seek to rebut this presumption by demonstrating that the cybersecurity expenditure does not meet one or more of the eligibility criteria (e.g., that, given the unique circumstances of the utility, the expenditure for which the utility seeks an incentive would not materially improve cybersecurity or is otherwise mandatory for that utility) or the Commission could make this finding *sua sponte*.

---

[23] *See* 18 CFR 388.113; *see also* 16 U.S.C. 824o-1.

27. We believe that this PQ List approach would provide efficiency and transparency benefits. With the Commission having pre-reviewed potential PQ List items, we believe that utility-specific incentive filings could be substantially streamlined compared to use of a case-by-case approach. We recognize, however, that this approach may 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, which introduces additional process and may delay the eligibility of cybersecurity expenditures for incentives.

i. <u>Initial PQ List</u>

28. We propose to include two eligible cybersecurity expenditures on the PQ List initially: (1) expenditures associated with participation in the DOE CRISP;[24] 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. We believe investment in these cybersecurity expenditures would materially improve cybersecurity;[25] and are not already mandated by CIP

---

[24] *See* DOE, *Energy Sector Cybersecurity Preparedness*, https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness.

[25] E.g., both participation in CRISP and internal network security monitoring would fall under recommendations in the NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations" catalog.

Reliability Standards[26] or otherwise mandated by Federal law. We initially propose 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.[27] However, we seek comments on whether to include other information sharing programs on the PQ List.

29. We propose to include internal network security monitoring on the PQ List as we believe that internal network security monitoring may better position an entity to detect malicious activity that has circumvented perimeter controls.[28] Further, while the currently effective CIP Reliability Standards do not require internal network security monitoring, NERC has recognized the proliferation and usefulness of such technology.[29]

---

[26] We note that, in January 2022, the Commission issued a NOPR that proposed to require NERC to develop a mandatory standard regarding internal network analysis and monitoring technologies for high and medium impact bulk electric system cyber systems. *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Notice of Proposed Rulemaking, 87 FR 4173 (Jan. 27, 2022), 178 FERC ¶ 61,038 (2022) (2022 INSM NOPR).

[27] DOE, *Energy Sector Cybersecurity Preparedness*, https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness.

[28] 2022 INSM NOPR at P 11.

[29] *See*, e.g., NERC, *ERO Enterprise CMEP Practice Guide: Network Monitoring Sensors, Centralized Collectors, and Information Sharing* (June 4, 2021),

30. Although we propose these two eligible cybersecurity expenditures for the initial PQ List, there may be other cybersecurity expenditures that would meet the statutory requirements and proposed eligibility criteria. Therefore, we seek comment on these and any additional cybersecurity expenditures to consider for inclusion on the initial PQ List

ii. Updating the PQ List

31. Considering the rapidly evolving nature of cybersecurity threats and solutions, we expect to regularly evaluate the PQ List and update it as necessary. The eligibility criteria described above, or any future eligibility criteria the Commission adopts, would guide the Commission's decision on what to add, modify, or remove from the PQ List. As noted above, we propose that, 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.[30] The Commission would update the PQ List by adding, removing, or modifying

https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf (explaining that NERC developed the guide in response to a U.S. DOE initiative "to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for [industrial control systems] of electric utilities." *Id.* at 1.).

[30] 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.

cybersecurity expenditures, as needed, via a rulemaking, whether *sua sponte* or in response to a petition.

b. Case-by-Case Approach

32. Another potential approach is to permit a utility to file for incentive-based rate treatment for any cybersecurity expenditure that satisfies the eligibility criteria discussed above, i.e., the utility could demonstrate 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. Under this approach, the Commission would review each filing on a case-by-case basis, to determine whether the proposed cybersecurity expenditure is consistent with the eligibility criteria. If the Commission adopts a case-by-case approach, there would be no presumption of eligibility for any given cybersecurity expenditure. The utility would bear the full burden to demonstrate in its filing that its cybersecurity expenditure meets the Commission-approved eligibility criteria, and, similar to the PQ list approach, demonstrate that its proposed rate, inclusive of the incentive, is just and reasonable. We seek comment on whether and, if so, how the Commission should implement a case-by-case approach.

B. Proposed Rate Incentives

33. We propose 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. We believe both offer meaningful incentive to encourage cybersecurity expenditure that improves a utility's cybersecurity posture. Additionally, we seek comment on whether and how the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.

34. Under Part II of the FPA, the Commission has jurisdiction over the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce by public utilities.[31] With limited exceptions, transmission rates are based on the cost of providing transmission service (cost-of-service rates). Cost-of-service transmission rates are recovered either through a formula rate, for which the formula is the rate on file and most of the inputs change year to year based on inputs that are included in the FERC Form No. 1 or other financial forms,[32] or a stated rate where the rate on file is based on an approved revenue requirement. Costs incurred to undertake cybersecurity

[31] 16 U.S.C. 824-824w. Unlike FPA section 219, titled Transmission Infrastructure Investment, which gives the Commission the authority to offer incentives for the transmission of electric energy in interstate commerce, new FPA section 219A, titled Incentives for Cybersecurity Investments, gives the Commission the authority to offer incentives for the transmission of electric energy in interstate commerce as well as the sale of electric energy at wholesale in interstate commerce by public utilities.

[32] *Doswell Ltd. P'ship v. Va. Elec. & Power Co.*, 62 FERC ¶ 61,149, at 62,069 (1993).

activities can be included in various accounting categories,[33] either as inputs to a formula rate as expenses or plant in the determination of the revenue requirement for a stated rate. The Commission has allowed costs related to security and reliability that are recovered through formula rates to include, for example, transmission plant (e.g., transmission line upgrades to harden the system), general and common plant, (e.g., software and computers), and administrative and general costs (e.g., labor and outside services, including services associated with utility-wide informational technology).[34] Utilities recover the cost of expenses as a cost-of-service element in rates, but do not earn a return on them. Utilities recover costs of capitalized investments through depreciation and earn a return on the undepreciated amounts over the useful life of the investment.[35]

35. Most utility information technology investments (general and intangible plant) and expenses (administrative and general costs) support functions of the

---

[33] In the Notice of Proposed Rulemaking in *Acct. & Reporting Treatment of Certain Renewable Energy Assets*, 180 FERC ¶ 61,050 (2022), the Commission proposes new accounts to more clearly specify how utilities must account for information technology hardware and software investments.

[34] *See Boston Edison Co.*, 109 FERC ¶ 61,300, at P 40 (2004), *order on reh'g*, 111 FERC ¶ 61,266 (2005) (accepting proposed modifications to transmission formula rates to allow recovery of capitalized software costs incurred to safeguard the reliability and security of its transmission system).

[35] The Commission has also accepted utility proposals to recover security costs as part of a utility's stated (i.e., non-formula) rates. *See Pacific Gas & Elec. Co.*, 149 FERC ¶ 61,112 (2014); *Pacific Gas & Elec. Co.*, 146 FERC ¶ 61,034 (2014).

entire utility, not just the transmission function, and therefore only a portion of those costs are allocated to transmission customers, typically based on wages and salaries allocators.[36]

1. ROE Adder

36. We propose to add § 35.48(e)(1) to the Commission's regulations to allow a utility that makes cybersecurity investments that are eligible for incentives, as more fully described above, to request an ROE adder of 200 basis points (Cybersecurity ROE Incentive) that would be applied to the incentive-eligible investments. Any incentive granted under this proposal would be subject to the total base and incentive return being capped at the top of the utility's zone of reasonableness.[37] This Cybersecurity ROE Incentive is intended to encourage utilities to proactively make additional investments in cybersecurity systems. We believe that a 200-basis point ROE adder may be appropriate to provide a meaningful incentive to encourage utilities to improve their systems' cybersecurity. We recognize that this amount exceeds the ROE incentives for

[36] *See*, *e.g.*, Midcontinent Independent System Operator Attachment O formula rate, 2-3 (stating that general and intangible plant and administrative and general costs are allocated to transmission rates based on a wages and salaries allocator).

[37] *See*, e.g.*, Emera Me. v. FERC*, 854 F.3d 9, 23 (D.C. Cir. 2017) ("The zone of reasonableness informs FERC's selection of a just and reasonable rate."); *see also Permian Basin*, 390 U.S. 747, 767 (1968) (stating that as long as the rate selected by the Commission is within the zone of reasonableness, the Commission is not required to adopt as just and reasonable any particular rate level).

transmission facilities that the Commission typically provides pursuant to FPA section 219. However, 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. On balance, we believe that the Cybersecurity ROE Incentive satisfies the Congressional directive to benefit consumers by encouraging: (1) investments by utilities in advanced cybersecurity technology; and (2) participation by utilities in cybersecurity threat information sharing programs.

37. We propose that enterprise-wide investments—which are not specific to transmission but a portion of which are recovered through transmission rates—may also be eligible for the 200 basis-point ROE adder incentive if the Commission determines that the investments merit incentives, based on the eligibility criteria described above. However, consistent with both longstanding cost-causation ratemaking principles[38] and the statutory requirement that rates inclusive of incentives be just and reasonable, we propose that only the conventionally allocated portion of such investments that flows through to cost-of-service rates on file with the Commission would be eligible for this rate treatment.

---

[38] *See Old Dominion Elec. Coop. v FERC,* 898 F.3d 1254, 1255 (D.C. Cir. 2018), ("For decades, the Commission and the courts have understood this requirement to incorporate a "cost-causation principle"—the rates charged for electricity should reflect the costs of providing it.); *see*, e.g., *Ala. Elec. Coop., Inc. v. FERC*, 684 F.2d 20, 27 (D.C. Cir. 1982).

For example, if a utility seeks an incentive for a cybersecurity investment that it made to its general plant facilities, both the underlying investment and associated incentive must be allocated based on conventions of the rates (e.g., the transmission share using a wages and salaries allocator for general plant in most transmission cost-of-service rates). With this limitation, we seek to ensure that the cybersecurity incentives policy adheres to the ratemaking principle of cost-causation by, for example, limiting a transmission customer's share of incentive costs to the share of such investments that serve transmission.

38. We preliminarily find that the same expenditure should not be eligible for both the Cybersecurity ROE Incentive and the Regulatory Asset Incentive, discussed below. Given that regulatory asset treatment may be approved for costs that are normally treated as expenses (i.e., as regulatory assets, discussed below), we preliminarily find 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.

2. **<u>Deferral of Certain Cybersecurity Expenses for Rate Recovery</u>**

39. We propose to add § 35.48(e)(2) to the Commission's regulations to allow a utility that makes cybersecurity investments that are eligible for incentives, as more fully described above, to seek deferred cost recovery. We believe that, in limited circumstances, it may be appropriate to allow a utility to defer recovery of certain cybersecurity costs that are generally expensed as they are incurred, and

treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base (Regulatory Asset Incentive). Many costs associated with cybersecurity are in the form of expenses, often to third party vendors, rather than capital investments. Moreover, certain cost categories that companies historically have purchased and capitalized, such as software, are now often procured as services with periodic payments to vendors that are recorded as expenses. Therefore, to encourage investment in cybersecurity, we believe that it may be appropriate to allow utilities to defer and amortize eligible costs that are typically recorded as expenses including those that are associated with third-party provision of hardware, software, and computing and networking services. We propose that eligible expenses, that would otherwise be includable in cost-of-service 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. Additionally, we seek comment on whether it would be preferable to permit only 50% of incentive-eligible expenses to be treated as regulatory assets.

40. A range of implementation costs associated with cybersecurity investments may be eligible for deferred rate treatment. Such costs may include, for example, training to implement new cybersecurity practices and systems. However, we propose that, to be eligible for the incentive of deferred cost recovery, such training costs must be distinct from costs associated with pre-existing training on cybersecurity practices. Another potentially eligible implementation cost may be

internal system evaluations and assessments or analyses by third parties described above, to the extent that they are associated with a capitalizable item and are part of eligible capitalizable expenses. We propose that any implementation costs that are not conventionally booked as plant and thus capitalized can be considered for deferral as a regulatory asset. Recurring costs may be eligible for deferral as a regulatory asset and include, for example, subscriptions, service agreements, and post-implementation training costs. Specifically, they may include ongoing dues for participation by utilities in cybersecurity threat information sharing programs that satisfy the Commission's incentive eligibility criteria described above.

41. Because FPA section 219A(c)(2) directs the Commission to offer incentives to encourage *participation* by public utilities in cybersecurity threat information sharing programs, we seek comment on whether we should allow utilities who are already participating in an eligible cybersecurity threat information sharing program to seek to recover this incentive.

42. We note that the Commission's rules and regulations in the Uniform System of Accounts[39] already require public utilities to maintain records supporting any entries to the regulatory asset account so that the public utility can furnish full information as to the nature and amount of, and justification for, each regulatory asset recorded in the account. Therefore, pursuant to our existing

[39] *See* 18 CFR part 101, Account Definition Account 182.3, Other Regulatory Assets, paragraph D.

regulations, utilities must maintain sufficient records to support the distinction of any expenditures that are afforded incentive-based rate treatment.[40]

43. Additionally, consistent with the proposal for the Cybersecurity ROE Incentive for eligible cybersecurity capital investments, we propose 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.

3. <u>Performance-Based Rates</u>

44. Section 219A(c) of the FPA directs the Commission to establish incentive-based, including performance-based, rate treatments. Performance-based rate treatments can potentially reward utilities for achieving stated goals, as opposed to specific actions that only contribute to those goals. Because it is difficult to directly observe the level of effort a utility expends on ensuring cybersecurity, performance-based regulation could theoretically provide a valuable tool to motivate utilities to maintain and operate their systems reliably and efficiently. Performance-based ratemaking can take multiple forms, but ultimately requires the ability to measure and tie rate treatments to actual performance.

45. We seek comment on performance-based rates and whether and how the principles of performance-based regulation could apply to utilities with respect to

[40] *Id.*

cybersecurity investments.[41] We seek comment on specific cybersecurity performance metrics that could be subject to a performance standard. In particular, we seek comment on 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. We further seek comment on what rate mechanisms could accompany such metrics. We ask that any proposed mechanisms: (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.

C. Proposed Incentive Implementation

1. Cybersecurity ROE Incentive Duration

46. We propose to add § 35.48(f)(1) to the Commission's regulations to allow a utility granted a Cybersecurity ROE Incentive to receive that incentive until the earliest of: (1) the conclusion of the depreciation life of the underlying asset; (2)

[41] 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).

five years from when the cybersecurity investment(s) enter service;[42] (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. 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. Thus, we believe that 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, we propose that the incentive end at the conclusion of five years from the time that the asset receiving the cybersecurity incentive entered service. The vast majority of information technology-related investments feature expected useful lives and corresponding cost-of-service depreciation rates of no longer than five years. Consequently, we preliminarily find that five years is a reasonable expected life to encourage utilities to make an investment and to ensure just and reasonable rates. However, we seek comment on whether the proposed duration should be three years instead of five years.

[42] For participation in an information sharing program, the “investment” would recur annually.

2. Regulatory Asset Incentive Duration and Amortization Period

47. We propose to add § 35.48(f)(3)(i) to the Commission's regulations to specify that a utility granted the Regulatory Asset Incentive must amortize the regulatory asset over five years.[43] We believe that this may reflect the generally short-lived nature of cybersecurity activities and corresponds to the depreciation rates for investments described above. This period generally corresponds to the expected useful life and corresponding cost-of-service amortization period of cybersecurity investments.

48. We also propose to add § 35.48(f)(3)(ii) to the Commission's regulations to specify that a utility granted the Regulatory Asset Incentive may defer eligible expenses for up to five years from the date of Commission approval of the incentive. Under this provision, we propose that 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, as discussed above.[44] We preliminarily find

[43] As noted above, the investment for participation in an information sharing program would recur annually.

[44] We propose that, in their FPA section 205 filings, incentive recipients must include notes to their formula rates specifying the Commission order(s) which approved the incentive and stating that the associated regulatory asset incentive must terminate in the earlier of: (1) five years from the date of the later of the Commission approving the incentive or the expense being incurred; and (2) the expenditure becoming mandatory.

that this limit is appropriate, given the potentially indefinite nature of certain expenses. Such a limit also reflects that cybersecurity risks and solutions evolve over time and matches the five-year maximum duration of the Cybersecurity ROE Incentive discussed above. We preliminarily find that a five-year limit appropriately balances the goal of providing an incentive of a sufficient size to encourage utilities to make eligible improvements in their cybersecurity posture with the requirement to protect ratepayers.

49. However, we propose to make an exception to this sunsetting provision for eligible cybersecurity threat information sharing programs. FPA section 219A(c)(2) directs the Commission to provide incentives for participation in cybersecurity threat information sharing programs. We find that participation in such cybersecurity threat information sharing programs, which provide participants with ongoing updates about active cybersecurity threats and are therefore distinct from discrete cybersecurity investments that may become obsolete with the passage of time, warrants a different incentive treatment than other investments. Consequently, we propose 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.

3. Filing Process

50. We propose to add § 35.48(g) to the Commission's regulations to require a utility's request for one or more incentive-based rate treatments to be made in a

filing pursuant to FPA section 205.[45] As proposed, such a request must include a detailed explanation of how the utility plans to implement one or both of the proposed incentive approaches and the requested rate treatment. We propose that utilities provide detail on the expenditures for which they seek incentives, and show how its cybersecurity-related expenditure(s) meet the eligibility requirements, as described in more detail below.

51. In addition, under § 35.48(g) of the proposed regulation, a utility seeking one or more incentive-based rate treatments must receive Commission approval prior to implementing any incentive in its rate on file with the Commission.[46] In order to effectuate an incentive in rates, utilities would need to propose in their FPA section 205 filing conforming revisions to their formula rates, as appropriate, to reflect incentive rate treatment granted pursuant to these proposed regulations.[47]

---

[45] As discussed in section III.A.2., consistent with our precedent for incentives under FPA section 219, while a utility may first file a petition for declaratory order to seek a ruling on its eligibility for an incentive, a utility still must make a filing under FPA section 205 for Commission review of any rate changes.

[46] We note that FPA section 219A(e)(2) expressly prohibits unjust and unreasonable double recovery for advanced cybersecurity technology.

[47] Utilities with stated rates may file under FPA section 205 to seek incentives as part of a larger rate case or make a request for single issue ratemaking, which the Commission will evaluate on a case-by-case basis to ensure that the rate, inclusive of the incentive, is just and reasonable.

52. Filings under the PQ List approach must provide evidence that the utility has made one or more pre-qualified cybersecurity expenditures and otherwise complies with all appropriate requirements.

53. A utility requesting the Cybersecurity ROE Incentive must provide the anticipated cost of the capital investment and the identity of the rate schedule(s) on file with the Commission under which it will recover the increased ROE. Alternatively, a utility requesting the Regulatory Asset Incentive must provide a description of the covered expense(s), including whether the expense(s) are associated with the third-party provision of hardware, software, and computing network services or incurred for training to implement network analysis and monitoring programs, as well as an estimate of the cost of such expense(s) and when the cost is expected to be incurred.

4. Reporting Requirements

54. In order to ensure that a utility receiving incentive rate treatment has implemented the requirements of the incentive and to ensure that it continues to adhere to the requirements, we propose to add § 35.48(h) of the Commission's regulations to require utilities to submit informational reports to the Commission for the duration of the incentive.

55. 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.[48] 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 Cybersecurity 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.

56. The Commission 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 (i.e., directing further informational filings, audits, etc.). The annual informational filings will inform the Commission on how and when any additional verification is warranted.

---

[48] 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.

IV. Information Collection Statement

57. The information collection requirements contained in this NOPR are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 at 44 U.S.C. 3507(d). OMB's regulations require approval of certain information collection requirements imposed by agency rules.[49] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this proposed rule will not be penalized for failing to respond to this collection of information unless the collection of information displays a valid OMB Control Number. This NOPR would establish the Commission's regulations with respect to the implementation of the Infrastructure and Job Act.[50]

58. Interested persons may obtain information on the reporting requirements by contacting Ellen Brown, Office of the Executive Director, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426 via email (DataClearance@ferc.gov) or telephone ((202) 502-8663).

59. The Commission solicits comments on this collection of information within 60 days of the publication of this NOPR in the *Federal Register*. Public comments may include, but are not limited to, following topics: the Commission's need for this information, whether the information will have practical utility, the

---

[49] 5 CFR 1320.11.

[50] Pub. L. 117-55, 135 Stat. 951 (2021) (to be codified at 16 U.S.C. 824s-1).

accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

60. Please send comments concerning the collection of information and the associated burden estimates to: OMB through www.reginfo.gov/public/do/PRAMain, Attention: Federal Energy Regulatory Commission Desk Officer. Please identify the OMB Control Number 1902-0248 in the subject line.

61. *Instructions:* OMB submissions must be formatted and filed in accordance with submission guidelines at: www.reginfo.gov/public/do/PRAMain; using the search function under the "Currently Under Review field," select Federal Energy Regulatory Commission, click "submit," and select "comment" to the right of the subject collection.

62. Title: FERC-725B, Incentives for Advanced Cybersecurity Investment.

63. Action: Proposed revision of FERC-725B.

64. OMB Control No.: 1902-0248

65. Respondents for this Rulemaking: Public utilities and non-public utilities that have or will have a rate on file with the Commission.

66. Frequency of Information Collection:

(1) On occasion: Voluntary filings seeking incentive-based rate treatment for cybersecurity expenditures; and

(2) Annually: A informational filing on June 1 of each year, required of entities that have been granted incentive-based rate treatment for cybersecurity expenditures.

67. Abstract: The NOPR would provide that a utility may seek incentive-based rate treatment for cybersecurity investments by making a rate filing in accordance with section 205 of the FPA. The NOPR states that one approach the Commission may use in evaluating such a filing is to consider whether prospective cybersecurity investments would match one of the types of investments listed at proposed 18 CFR 35.48(d). The NOPR refers to this list of pre-qualified expenditures that are eligible for incentives as the "PQ List." The Commission proposes that any cybersecurity expenditure that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive.

The NOPR also discusses and seeks comment on a potential alternative approach, in which a utility's cybersecurity expenditure would be evaluated on a case-by-case basis to determine if it is eligible for an incentive. Under that approach, the utility would need to demonstrate that the prospective investment is voluntary and would materially improve cybersecurity through either an investment in advanced cybersecurity technology or participation in cybersecurity threat information sharing program. Under either approach, the utility would need to demonstrate that its rate, inclusive of the incentive, is just and reasonable.

68. The NOPR also would provide that a utility that is granted incentive-based rate treatment must submit an annual informational filing to the Commission by

June 1 of each year, provided that the utility has received Commission approval of the incentive at least 60 days prior to June 1 of that year. Utilities that receive Commission approval of 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. The informational filing must describe 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 incentives where the Commission allows deferral of expenses, annual informational filings should describe such expenses in sufficient detail to demonstrate that such expenses are specifically related to the cybersecurity investment for which the incentive was granted, and not for ongoing services including system maintenance, surveillance, and other labor costs.

69. Necessity of Information: Required to obtain or retain benefits.

70. Internal Review: The Commission has reviewed the changes and has determined that such changes are necessary. These requirements conform to the Commission's need for efficient information collection, communication, and management within the energy industry. The Commission has specific, objective support for the burden estimates associated with the information collection requirements.

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. The Commission estimates that the NOPR may affect the burden[51] and cost[52] as follows:

FERC-725B, **Proposed Changes in NOPR in Docket No. RM22-19-000**					
A. Area of Modification	**B. Number of Respondents**	**C. Annual Estimated Number of Responses per Respondent**	**D. Annual Estimated Number of Responses (Column B X Column C)**	**E. Average Burden Hours & Cost ($) per Response**	**F. Total Estimated Burden Hours & Total Estimated Cost ($) (Column D x Column E)**
Voluntary filing seeking incentive rate treatment for cybersecurity investment. Proposed 18 CFR 35.48(b).	50	1	50	80 hours; $7,280	4,000 hours; $364,000
Annual informational filing required where Commission has granted incentive rate treatment. Proposed 18 CFR 35.48(h).	50	1	50	40 hours; $3,640	2,000 hours; $182,000
Totals					**6,000 hours; $546,000**

[51] "Burden" is the total time, effort, or financial resources expended by persons to generate, maintain, retain, or disclose or provide information to or for a Federal agency. For further explanation of what is included in the information collection burden, refer to 5 CFR 1320.3.

[52] Commission staff estimates that respondents' hourly wages (including benefits) are comparable to those of FERC employees in Fiscal Year 2022. Therefore, the hourly cost used in this analysis is $91 and $188,992 annually.

V. Environmental Assessment

72. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect on the human environment.[53] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[54] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Regulatory Flexibility Act

73. The Regulatory Flexibility Act of 1980[55] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) sets the threshold for what constitutes a small business. Under SBA's size standards,[56] transmission owners all fall under the category of Electric Bulk Power Transmission and Control (NAICS code 221121), with a size threshold of 500

---

[53] *Reg'ls. Implementing the Nat'l. Env'nt. Pol'y Act*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

[54] 18 CFR 380.4(a)(2)(ii).

[55] 5 U.S.C. 601-612.

[56] 13 CFR 121.201.

employees (including the entity and its associates).[57] The NERC Compliance Registry, as of August 5, 2022, identifies approximately 1,669 utilities, both public and non-public, in the U.S. that potentially would be affected by the voluntary information collection associated with the proposed incentive and rate treatment in this NOPR. Based on the Compliance Registry, we have reviewed a randomly selected sample of 92 entities, and we have determined that approximately 80% of the listed entities are small entities (i.e., with fewer than 500 employees).

74. Regarding information collection activities, we estimate an average one-time cost of $7,280 for each of 50 new filers, and an average annual cost of $3,640 for each of 50 continuing recipients of rate incentives.

75. According to SBA guidance, the determination of significance of impact "should be seen as relative to the size of the business, the size of the competitor's business, the number of filers received annually, and the impact this regulation has on larger competitors."[58]

76. Moreover, this NOPR involves voluntary actions by utilities for the purpose of benefitting consumers by encouraging investments by utilities in advanced cybersecurity technology and participation by utilities in cybersecurity threat

---

[57] The threshold for the number of employees indicates the maximum allowed for a concern and its affiliates to be considered small.

[58] U.S. Small Business Administration, *A Guide for Government Agencies How to Comply with the Regulatory Flexibility Act*, 18 (May 2012), https://www.sba.gov/sites/default/files/advocacy/rfaguide_0512_0.pdf.

information sharing programs. The proposal does not mandate or require action by any utility. As a result, we certify that the proposals in this NOPR will not have a significant economic impact on a substantial number of small entities.

VII. Comment Procedures

77. The Commission invites interested persons to submit comments on the matters and issues proposed in this NOPR to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due 30 days after the date of publication in the *Federal Register*, and reply comments are due 45 days after the date of publication in the *Federal Register*. Any comment must refer to Docket No. RM22-19-000, and must include the commenter's name, the organization it represents, if applicable, and its address in its comments. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

78. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's website at https://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software must be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

79. Commenters that are not able to file comments electronically may file an original of their comments by USPS mail or by courier-or other delivery services. For submission sent via USPS only, filings should be mailed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street, NE, Washington, DC 20426. Submission of filings other than by USPS should be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

VIII. Document Availability

80. In addition to publishing the full text of this document in the *Federal Register*, the Commission provides all interested persons with an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (https://www.ferc.gov).

81. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this number in the docket number field.

82. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at 202-502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202)502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

List of subjects in 18 CFR Part 35

Electric power rates, Electric utilities, Reporting and recordkeeping requirements.

By direction of the Commission. Commissioner Phillips is concurring with a separate statement attached.

Issued: September 22, 2022.

Debbie-Anne A. Reese,

Deputy Secretary.

In consideration of the foregoing, the Commission proposes to amend part 35, chapter I, title 18, Code of Federal Regulations, as follows:

PART 35 – FILING OF RATE SCHEDULES AND TARIFFS

1. The authority citation for part 35 continues to read as follows:

Authority: 16 U.S.C. 791a-825r, 2601-2645; 31 U.S.C. 9701; 42 U.S.C. 7101-7352.

2. Add subpart K, consisting of § 35.48, to read as follows:

Subpart K – Cybersecurity Investment Provisions

§ 35.48 Cybersecurity investment.

(a) *Purpose.* This section establishes rules for incentive-based rate treatments for utilities that voluntarily make cybersecurity investments as described in this section.

(b) *Incentive-based rate treatment for cybersecurity investment*. The Commission will authorize incentive-based rate treatment for a utility that voluntarily makes an investment in advanced cybersecurity technology and for a utility that voluntarily participates in a cybersecurity threat information sharing program under this section. Incentive-based rate treatment is available to both public and non-public utilities that have or will have a rate on file with the Commission. A utility may request incentive-based rate treatment for an eligible cybersecurity investment that meets the eligibility criteria set forth in paragraph (c) of this section.

(c) *Eligibility criteria*. A utility may receive incentive-based rate treatment for a cybersecurity investment that:

(1) Materially improves cybersecurity through either investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program; and

(2) Is not already mandated by the mandatory and enforceable Critical Infrastructure Protection Reliability Standards as maintained by the Electric Reliability Organization, or otherwise mandated by local, state, or Federal law. A utility may receive incentive-based rate treatment for the investment pursuant to paragraphs (d) through (h) of this section.

(d) *Pre-qualified cybersecurity expenditure*. A utility must demonstrate that a cybersecurity expenditure qualifies as one or more of the pre-qualified cybersecurity expenditures identified by the Commission pursuant to this paragraph (d). A utility should seek critical energy/electric infrastructure information treatment with the Commission, as appropriate, for any part of its filing seeking incentive-based rate treatment that has specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure. Pre-qualified cybersecurity expenditures include:

(1) Expenditures associated with participation in the Department of Energy's Cybersecurity Risk Information Sharing Program.

(2) Expenditures associated with internal network security monitoring within the utility's cyber systems.

(e) *Types of incentive-based rate treatment for cybersecurity investment.* For purposes of paragraph (b) of this section, incentive-based rate treatment shall mean either of the following:

(1) An increase in rate of return on equity of 200 basis points that would be applied to the incentive-eligible investment; or

(2) Deferral of expenses as a regulatory asset;

(f) *Incentive duration.* (1) A return on equity incentive-based rate treatment approved pursuant to this section shall last no longer than the earliest of:

(i) The depreciation life of the underlying asset;

(ii) Five years from when the cybersecurity investment enters service;

(iii) When the cybersecurity investment or activity that serves as the basis of that incentive becomes mandatory; or

(iv) When the utility no longer meets the requirements for receiving the incentive.

(2) An incentive granted for participation in a qualified cybersecurity threat information sharing program will not be subject to a sunset, such that a utility participating in a qualified cybersecurity threat information sharing program is eligible to continue deferring expenses associated with membership, which for each year would be amortized over the next five years, for as long as it is a member and participation is not mandatory.

(3) A deferred regulatory asset whose costs are typically expensed should be:

(i) Amortized over a five-year period; and

(ii) Limited to expenses incurred in the first five years following Commission approval of the incentive.

(g) *Incentive applications.* For the purpose of paragraphs (b) and (c) of this section, a utility's request for one or more incentive based-rate treatments, to be made in a filing pursuant to section 205 of the Federal Power Act, must include a detailed explanation of the proposed rate treatment and include the following information:

(1) Evidence that it has made one or more pre-qualified cybersecurity expenditures and otherwise complies with all requirements of this section.

(2) For applications requesting an increase in rate of return on equity of 200 basis points:

(i) The anticipated cost of the capital investment; and

(ii) The identity of the rate schedule(s) on file or to be filed with the Commission under which it will recover the increased return on equity.

(3) For applications requesting deferred cost recovery:

(i) A description of any expenses, including whether the expenses are:

(A) Expenses associated with third-party provision of hardware, software, and computing networking services; and/or

(B) Expenses for training to implement network analysis and monitoring programs;

(ii) Estimates of the cost of such expenses; and

(iii) When the costs are expected to be incurred.

(h) *Reporting requirements*. A utility that has received an incentive under this section must make an annual informational filing on June 1, provided that the utility has received Commission-approval for the incentive at least 60 days prior to June 1 of that year. The annual filing should detail the specific investments that were made pursuant to the Commission's approval and the corresponding FERC account used. A utility that has received an incentive under this section must describe any parts of its network that it upgraded in addition to the nature and cost of the various investments. For incentives where the Commission allows deferral of expenses, annual informational filings should describe such expenses in sufficient detail to demonstrate that such expenses are specifically related to the cybersecurity investment granted incentives and not for ongoing services including system maintenance, surveillance, and other labor costs.

Note: The following appendix will not appear in the Code of Federal Regulations.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Incentives for Advanced Cybersecurity Investment Docket Nos. RM22-19-000
RM21-3-000

PHILLIPS, Commissioner, *concurring*:

1. I concur in today's Notice of Proposed Rulemaking[1] to highlight the importance of today's action and to encourage stakeholder comment in certain areas. In today's highly interconnected world, the nation's security and economic well-being depends on reliable and cyber-resilient energy infrastructure. This is why it is critical that we continue to build upon the mandatory framework that the industry has already identified through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. But, these mandatory CIP standards are just a baseline and can take years to implement. Recent cyber-attacks in Ukraine and here at home remind us of the constant threat of foreign and domestic attacks on our critical infrastructure, and the need for advanced and innovative technology and threat information sharing programs for emerging threats. Therefore, I fully support this action we are taking under section 219A of the Federal Power Act (FPA)[2] to encourage utilities to proactively make additional cybersecurity investments in their systems.

2. There are significant costs when there is a cybersecurity breach on the electric or gas system. Not only are consumers impacted by loss of service, but the recovery costs are significant. For example, the Colonial Pipeline cybersecurity breach effectively shut down half of the country's fuel supply, and even though the pipeline invested $200 million dollars over five years to contain a

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

[2] 16 U.S.C. 824s-1.

potential attack,[3] Colonial Pipeline still spent millions more to recover from the event in 2021.[4]

3. This NOPR serves as a critical step to incent public and non-public utilities to make urgent cybersecurity investments in advanced technology. First, the NOPR proposes to incentivize expenditures that materially improve the cybersecurity posture of utilities.[5] Second, the NOPR provides that those cybersecurity investments must not already "be mandated by [CIP] Reliability Standards, or local, state, of federal law."[6] Third, the NOPR proposes that the Commission either use a pre-qualified (PQ) list of approved cybersecurity expenditures, where any expenditures that meet the list would be entitled to a rebuttable presumption that the utility is eligible for an incentive,[7] or that the Commission assess expenditures on a case-by-case basis.[8] Lastly, the NOPR proposes that if a utility meets the requirements for an incentive, it could either receive a return on equity (ROE) adder of 200 basis points or deferred cost recovery for expenditures that enables the utility to defer expenses and include the unamortized portion in rate base.[9] All of these items are essential to improving utilities' ability to protect, detect, respond to, and recover from a cybersecurity threat.

4. Specifically, I am interested in feedback on whether the proposed PQ list is broad enough to include all expenditures that may warrant incentives. As proposed, if an expense is associated with participation in the Cybersecurity Risk

---

[3] *See* Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure, Hearing Before the Committee on Homeland Security, 117th Cong. (2021) (Statement of Joseph A. Blount).

[4] *See Everhart v. Colonial Pipeline Company*, 2022 WL 3699967, (N.D. Ga. 2022) ("Colonial paid the cybercriminals . . . a $4.4 million ransom in return for a decryption tool that allowed Colonial to retrieve the encrypted or locked data.").

[5] NOPR at PP 2, 20, 22.

[6] NOPR at PP 2, 22.

[7] NOPR at PP 3, 19; *see infra* at PP 4-5.

[8] NOPR at PP 3, 19, 22-23.

[9] NOPR at PP 4, 34, 37.

Sharing Program (CRISP)[10] or if an expenditure is associated with internal network security monitoring within the utility's cyber systems,[11] there would be a rebuttable presumption that that expense is entitled to an incentive. I agree that each eligible cybersecurity expenditure on the PQ list should have a single, clear, and non-trivial benchmark that must be met for a utility to qualify for incentive rate treatment. But, the proposed PQ list is limited. For example, 75% of electricity customers in the continental U.S. are served by investor-owned utilities that already participate in CRISP,[12] which demonstrates the limited potential benefits from this incentive. Under the NOPR proposal, it is unclear whether a utility that already participates in CRISP could receive an incentive for future subscription costs for continued CRISP participation. I encourage comments on whether any final rule should clarify that such continued CRISP participation is indeed entitled to an incentive.

5. I also recognize that a case-by-case approach, as opposed to the proposed PQ list, would be more adaptable and less prescriptive, allowing a variety of solutions that utilities could potentially tailor to their specific situations. However, given the diverse and evolving nature of cybersecurity activities, this option could be very time-consuming and administratively inefficient. Thus, I believe that an expanded PQ list is a reasonable approach that would satisfy the applicable statutory directives while providing a high degree of certainty for regulated entities. I urge all interested stakeholders to provide comments on whether the Commission should widen the PQ list's universe of potential expenditures. I especially encourage stakeholders to comment on whether the Commission should

---

[10] Co-funded by the Department of Energy (DOE) and industry and managed by E-ISAC, CRISP is a public-private partnership that enables and manages the near real-time sharing of IT network information between electricity utilities and key DOE resources. The purpose of CRISP is to enable collaboration among energy sector partners 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.

[11] The Commission issued a NOPR that proposed to direct NERC to develop a mandatory standard regarding internal network security monitoring in the context of high and medium impact bulk electric system. *See Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, 178 FERC ¶ 61,038 (2022).

[12] *See Energy Sector Cybersecurity Preparedness*, available at: https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness.

consider external penetration tests, a security awareness program, a patch management program, and/or the capability to disconnect operational technology from the information technology network for the PQ list.

6. I also want to underscore the need for utilities to conduct analyses of electric and gas interdependencies, and how such actions would benefit cybersecurity on the bulk electric system. I fully recognize that FPA section 219A states that the Commission can establish "incentive-based, including performance-based, rate treatments for the transmission of *electric energy in interstate commerce*,"[13] and the Infrastructure Act only modified section 219 regarding incentives and not the Natural Gas Act (NGA).[14] However, electric and gas companies are especially vulnerable to cyberattacks, particularly because utilities that use both sources have an expansive and increasing attack surface, arising from their geographic and organizational complexity. Indeed, the electric and gas sector's unique interdependencies increase their vulnerability to exploitation, which can include the commandeering of the operational-technology system to stop energy infrastructure from working at times when consumers most need it. To the extent we can identify the need for cybersecurity information sharing between the natural gas and electric systems, and incentivize participation in such a program, I encourage stakeholder comment.

7. I further urge stakeholders to comment on whether the proposed duration of the incentives is sufficient and whether a 200-basis point adder is reasonable, as the NOPR contemplates.[15] To be clear, I do not support open-ended or permanent cyber incentives. I believe the 5-year proposed duration and the 200-basis point adder are adequate to properly incent utilities. Unlike expenses in the traditional

---

[13] 16 U.S.C. § 824s-1(c) (emphasis added).

[14] The Infrastructure Investment and Jobs Act (Infrastructure Act) modified Section 219 of the FPA regarding electric energy rate treatments and directed the Commission to consider incentives for the transmission of electric energy regarding cybersecurity. Section 219 did not, however, explicitly reference or modify the NGA regarding gas incentives.

[15] NOPR at PP 4, 33, 36-37; *see, e.g.*, Initial Comments of Edison Electric Institute., Docket No. RM21-3-000, at 2 (filed April 6, 2021) ("EEI agrees that given the relatively low dollar amounts associated with cybersecurity investments . . . the proposed 200 basis point cap is reasonable."); Comments of MISO Transmission Owners, Docket No. RM21-3-000, at 9 (filed April 6, 2021) (explaining why inclusion of enterprise-wide costs is appropriate to incent investment in critical facilities).

transmission incentives context,[16] the dollar amounts in cybersecurity investments are typically small. Yet, the benefits of additional, advanced cybersecurity investments cannot be ignored. Offering anything less than what is proposed would likely be insufficient to incent any action by utilities, as required by Congress. Therefore, commenters should provide specific, compelling reasons if they oppose the NOPR proposal regarding the duration of the incentive and the amount added to a utility's ROE.

8. Finally, I note that for years now, the White House, the U.S. Congress, and senior government leaders have sounded the alarm on increasing cybersecurity threats and their sophistication.[17] I also note that the Commission began assessing

---

[16] Brattle-Grid Strategies Oct. 2021 Report at 2 (citing Johannes Pfeifenberger & John Tsoukalis, The Brattle Group, *Transmission Investment Needs and Challenges*, at slide 2 (June 1, 2021), https://www.brattle.com/wp-content/uploads/2021/10/Transmission-Investment-Needs-and-Challenges.pdf); Johannes Pfeifenberger et al., The Brattle Group, *Cost Savings Offered by Competition in Electric Transmission: Experience to Date and the Potential for Additional Customer Value*, at 2-3 & fig.1 (Apr. 2019), available at: https://www.brattle.com/wp-content/uploads/2021/05/16726_cost_savings_offered_by_competition_in_electric_transmission.pdf (Brattle Apr. 2019 Competition Report).

[17] For example, President Biden told utilities and other companies that "critical infrastructure owners and operators must accelerate efforts to lock their digital doors." *See Statement by President Biden on Our Nation's Cybersecurity*, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity. President Biden has also since announced an executive order on cybersecurity and is using funds from the Infrastructure Act to provide grants to state, local, and territorial governments as they respond to cyber threats. *See* Exec. Order No. 14,028, 86 FR 26633 (2021). Former President Obama declared that cybersecurity threats are "the most serious economic and national security challenge[] we face as a nation" and that "America's economic prosperity . . . will depend on cybersecurity." *See* National Security Council, *Cyber Security*, available at: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity. Former Defense Secretary Leon Panetta warned that the country is "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid." *See* Elizabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattacks on U.S.*, The New York Times, October 11, 2021, available at: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

the potential use of incentives to improve cybersecurity prior to the passage of the Infrastructure Act.[18] While we are terminating the proceeding in Docket No. RM21-3-000, I am heartened that the Commission remains committed to this issue. I look forward to examining all the comments as we seek to issue a final rule around these topics.

For these reasons, I respectfully concur.

____

Willie L. Phillips
Commissioner

[FR Doc. 2022-21003 Filed: 10/5/2022 8:45 am; Publication Date: 10/6/2022]

[18] *See, e.g.,* FERC, *Cybersecurity Incentives Policy White Paper*, Docket No. AD20-19-000, (June 2020), available at: https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf (discussing the potential new framework for providing transmission incentives to utilities for cybersecurity investments); *Cybersecurity Incentives*, 87 FR 4173 (Jan. 27, 2021), 173 FERC ¶ 61,240 (2020) (proposing to allow utilities to request incentives for certain cybersecurity investments that go above and beyond the requirements of the CIP reliability standards). This NOPR supersedes the *Cybersecurity Incentives* NOPR, but it illustrates my colleagues' commitment to building out a more resilient electric system.