DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 35

[Docket No. RM22–19–000; Order No. 893]

Incentives for Advanced Cybersecurity Investment

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission is revising its regulations to provide incentive-based rate treatment 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.

DATES: This rule is effective July 3, 2023.

FOR FURTHER INFORMATION CONTACT:

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*.

Ryan Maca (Technical Information), Office of Energy Infrastructure Security, Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426, (202) 502–6129, *ryan.maca@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 J. 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 final rule, the Federal Energy Regulatory Commission revises its regulations pursuant to section 219A of the Federal Power Act (FPA) [1] to add subpart K, consisting of § 35.48, to our regulations to establish rules for incentive-based rate treatment for certain voluntary cybersecurity investments [2] by utilities [3] as described in this final rule. These rules make incentive-based rate treatment available to utilities that make voluntary cybersecurity investments in Advanced Cybersecurity Technology [4] that

[1] Infrastructure Investment and Jobs Act of 2021, Public Law 117–58, section 40123, 135 Stat. 429, 951 (to be codified at 16 U.S.C. 824s–1) (IIJA).

[2] In this final rule, the term investments includes expenditures that can be either capitalized costs or expenses.

[3] Notwithstanding that FPA section 219A requires the Commission to offer incentives to public utilities, as discussed in section III.A.1. of this final rule, we make rate incentives also 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. We intend that all references in this final rule to utilities include both public utilities and non-public utilities that have or will have a rate on file with the Commission.

[4] 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

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. The Commission is issuing this final rule to comply with FPA section 219A(c).[5] This voluntary cybersecurity incentive-based rate treatment is for the purpose of benefitting consumers by encouraging cybersecurity investments in Advanced Cybersecurity Technology and in participation in cybersecurity threat information sharing programs.[6]

2. We establish a regulatory framework for utilities to request incentive-based rate treatment for certain voluntary cybersecurity investments.[7] Under this framework, we: (1) identify the utilities permitted to request incentive-based rate treatment for cybersecurity investments; (2) establish the criteria that the Commission will use to determine whether a cybersecurity investment is eligible to receive an incentive-based rate treatment; (3) discuss the approaches that a utility may use to demonstrate that a cybersecurity investment satisfies the eligibility criteria; (4) explain the types of incentive-based rate treatments available for qualifying cybersecurity investments; (5) set limits on the duration of the incentive-based rate treatment; (6) describe what utilities must include in their applications for incentive-based rate treatment for cybersecurity investments; and (7) establish the annual reporting requirements for utilities that receive incentive-based rate treatment for their cybersecurity investments.

II. Background

A. Infrastructure Investment and Jobs Act of 2021

3. On November 15, 2021, the IIJA was signed into law.[8] Section 40123 of the IIJA added section 219A to the FPA, which 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 utilities in Advanced Cybersecurity Technology and participation by public utilities in cybersecurity threat information sharing programs.

1. Advanced Cybersecurity Technology

4. Under FPA section 219A(a), an Advanced Cybersecurity Technology can be a product and/or a service.[9] Cybersecurity products are generally hardware, software, and cybersecurity services that can be used for information technology (IT) systems and/or operational technology (OT) systems.[10] 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.

5. 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.

6. Under FPA section 219A(a), 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. FPA section 219A(g) states that Advanced Cybersecurity Technology Information that is provided to, generated by, or collected by the Federal Government under FPA section 219A subsections (b), (c), or (f) shall be considered to be critical electric infrastructure information under FPA section 215A.[11] Utilities submitting to the Commission Advanced Cybersecurity Technology Information or other information they believe to be Critical Energy/Electric Infrastructure Information (CEII) must clearly indicate which portions of their filing contains CEII and provide public and non-public versions of the information pursuant to the Commission's regulations.[12]

2. Cybersecurity Threat Information Sharing Programs

7. FPA section 219A(c) directs the Commission to identify incentive-based rate treatments that could support participation by public utilities in cybersecurity threat information sharing programs. Utilities face barriers to participating in cybersecurity information sharing programs, such as 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 cybersecurity threat information sharing programs, and concerns regarding the confidentiality of the information once shared.

B. Study and Report to Congress

8. As an initial step in the process of revising the Commission's regulations, FPA section 219A(b) requires the Commission to conduct a study, in consultation with certain entities,[13] 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

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. IIJA, Public Law 117–58, section 40123, 135 Stat. at 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)).

[5] IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(c)).

[6] *Id.*

[7] *Incentives for Advanced Cybersecurity Investment,* Notice of Proposed Rulemaking, 87 FR 60567 (Oct. 6, 2022), 180 FERC ¶ 61,189 (2022) (NOPR).

[8] IIJA, Public Law 117–58, 135 Stat. 429.

[9] *Id.* at 952 (to be codified at 16 U.S.C. 824s–1(c)).

[10] The National Institute of Standards and Technology (NIST) glossary defines OT to mean 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.*

[11] IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(g)) (citing 16 U.S.C. 824o–1).

[12] *See* 18 CFR 388.113(d)(1)(i)–(ii).

[13] FPA section 219A(b) identifies the following entities: the Secretary of Energy; North American Electric Reliability Corporation (NERC); Electricity Subsector Coordinating Council (ESCC); and National Association of Regulatory Utility Commissioners (NARUC).

information sharing programs.[14] As directed, Commission staff consulted with the specified entities to help identify incentive-based rate treatments that could enhance the security posture of the Bulk-Power System.[15]

9. In addition to conducting the study, FPA section 219A(b) requires the Commission to submit a report to Congress (Report) detailing the results of the study. On May 13, 2022, the Report was submitted to Congress.[16] 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.

C. NOPR

10. On September 22, 2022, the Commission issued the NOPR in this proceeding, proposing under FPA section 219A to establish rules for incentive-based rate treatments for certain voluntary cybersecurity investments by utilities.[17] The Commission proposed that these rules would make incentives available to utilities that make certain cybersecurity investments that enhance their security posture by improving their ability to protect against, detect, respond to, or recover from a cybersecurity threat, or that participate in cybersecurity threat information sharing programs to the benefit of ratepayers and national security.

11. First, the Commission proposed a regulatory framework for how a utility could qualify for incentives for eligible cybersecurity investments.[18] Under this framework, the Commission proposed that eligible cybersecurity investments must: (1) materially improve cybersecurity through either an investment in Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program; [19] and (2) not already be mandated by Critical Infrastructure Protection (CIP) Reliability Standards, or local, State, or Federal law.[20] The Commission proposed that a utility would seek incentive-based rate treatment for a cybersecurity investment in a filing pursuant to FPA section 205,[21] and that the incentive would be effective no earlier than the date of the Commission order approving the incentive request.[22]

12. Second, the Commission proposed to evaluate cybersecurity investments using a list of pre-qualified expenditures that are determined by the Commission to be eligible for incentives, which would be posted on the Commission's public website (PQ List).[23] The Commission proposed that any cybersecurity investment that is on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive.[24] With the Commission having evaluated cybersecurity investments to include on the PQ List in advance of the application for incentive-based rate treatment, along with the rebuttable presumption, the Commission postulated that the PQ List approach would provide an efficient and transparent mechanism for determining appropriate cybersecurity investments that are eligible for incentives.[25] The Commission also discussed and sought comment on a potential alternative approach, whereby a utility's cybersecurity investment would be evaluated on a case-by-case basis to determine if it is eligible for an incentive.[26]

13. Third, the Commission proposed two potential cybersecurity incentives: (1) a return on equity (ROE) adder of 200 basis points (Cybersecurity ROE Incentive); [27] and (2) deferred cost recovery for certain cybersecurity investments that enables the utility to defer expenses and include the unamortized portion in its rate base (Cybersecurity Regulatory Asset Incentive).[28]

14. Fourth, the Commission proposed that any approved incentive(s) would remain in effect for five years from the date on which the cybersecurity investment(s) enters service or the expenses are incurred, or expire earlier if certain other conditions discussed in the NOPR are met before the end of that five year period, *e.g.,* the cybersecurity investment becomes mandatory.[29] For continued voluntary participation in a cybersecurity threat information sharing program, however, the Commission proposed 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.[30] The Commission sought comment on the proposed duration and expiration conditions for incentives granted under this proposal.

15. Finally, the Commission proposed that a utility receiving a cybersecurity incentive pursuant to the proposed rule must make an annual informational filing by June 1 of each year following the receipt of incentive for as long as the utility receives the incentive.[31] The Commission proposed that the annual filing should detail the specific cybersecurity investments that were made pursuant to the Commission's approval and the corresponding FERC account used.[32]

16. The initial comment period for the NOPR ended on November 7, 2022, and the Commission received 27 initial comments. The reply comment period for the NOPR ended on November 21, 2022, and the Commission received six reply comments.

III. Discussion

17. To implement the statutory directive in FPA section 219A, we add subpart K to our regulations, consisting of § 35.48, to establish the rules for incentive-based rate treatment for utilities that voluntarily make cybersecurity investments as described in this final rule. For this final rule, a

[14] IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(b)).

[15] 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). In the context of developing and determining the applicability of mandatory Reliability Standards, NERC uses the term bulk electric system, which NERC defines to generally include the 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 (Mar. 8, 2023), *https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf* (NERC Glossary).

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

[17] NOPR, 180 FERC ¶ 61,189 at P 1.

[18] *Id.* P 2.

[19] *Id.* PP 20–22.

[20] *Id.*

[21] 16 U.S.C. 824d. The Commission noted that a utility would be permitted to first file a petition for declaratory order to seek a Commission determination on its eligibility for an incentive, but the utility would still need to make a filing with the Commission pursuant to FPA section 205 before adding the incentive-based rate treatment to its rate on file with the Commission.

[22] NOPR, 180 FERC ¶ 61,189 at P 24.

[23] *Id.* P 25.

[24] *Id.* P 26.

[25] *Id.* P 27.

[26] *Id.* P 32.

[27] *Id.* P 36.

[28] *Id.* P 39.

[29] *Id.* PP 46–49.

[30] *Id.* P 49.

[31] *Id.* PP 54–56.

[32] *See* 18 CFR pt. 141.

cybersecurity investment includes both expenses and capitalized costs associated with Advanced Cybersecurity Technology and participation in a cybersecurity threat information sharing program. In this final rule we: (1) identify the utilities permitted to request incentive-based rate treatment for cybersecurity investments; (2) establish the criteria that the Commission will use to determine whether a cybersecurity investment is eligible to receive an incentive-based rate treatment; (3) discuss the approaches that a utility may use to demonstrate that a cybersecurity investment satisfies the eligibility criteria; (4) explain the type of incentive-based rate treatment available for qualifying cybersecurity investments; (5) set limits on the duration of the incentive-based rate treatment; (6) describe what utilities must include in their applications for incentive-based rate treatment for cybersecurity investments; and (7) establish the annual reporting requirements for utilities that receive incentive-based rate treatment for their cybersecurity investments.

A. Cybersecurity Investments

18. We establish a structure that allows certain entities to request rate incentives for cybersecurity investments that satisfy the eligibility criteria. First, we determine which utilities may request the cybersecurity incentives. Next, we add definitions that identify the types of investments for which those utilities could seek incentive-based rate treatment. Finally, we establish the eligibility criteria that the Commission will use to determine whether a cybersecurity investment is eligible for an incentive.

1. Utilities Eligible To Request Rate Incentives for Cybersecurity Investments

19. FPA section 219A(c) directs the Commission to establish, by rule, incentive-based rate treatment 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 benefiting consumers by encouraging cybersecurity investments.[33]

a. NOPR Proposal

20. In the NOPR, the Commission proposed to make rate incentives available to both public utilities as well as non-public utilities that have or will have a rate on file with the Commission, similar to Commission precedent regarding transmission incentives under FPA section 219.[34] The Commission explained that it intended that all references to utilities in the NOPR would include both public utilities and non-public utilities that have or will have a rate on file with the Commission.

b. Comments

21. Some commenters discuss the utilities that should or should not be eligible for cybersecurity incentives. American Public Power Association (APPA) agrees with the NOPR proposal that non-public utilities with rates on file with the Commission should be eligible to receive incentives for qualifying investments.[35] Electric Power Supply Association (EPSA) also supports the proposal and argues that the statutory language in FPA section 219A requires the Commission to extend the proposed incentives to all utilities whose rates are regulated by the Commission, including those utilities who recover their costs through competitive markets.[36]

22. EPSA contends that Congress did not intend to limit cybersecurity incentives to utilities with cost-of-service rates on file with the Commission, but rather intended to make incentive-based rates available to all utilities, including those with market-based rates.[37] EPSA specifically suggests that the Commission establish formula rates for costs associated with identified incented cybersecurity investments. Alternatively, EPSA suggests allowing market-based rate entities to make FPA section 205 filings to recover the costs of eligible cybersecurity investments.[38] In contrast, California Public Utilities Commission and the California Department of Water Resources State Water Project (California Parties) suggest that market-based rate sellers or generators should not be eligible for incentives, so as to avoid interference with competitive markets.[39] Transmission Access Policy Study Group (TAPS) states that the Commission should explicitly exclude generators with market-based rates from incentive eligibility.[40] APPA urges the Commission to clarify in the final rule that its proposed incentives are limited to cost-based rates and not available for wholesale sales made under market-based rate authority.[41]

c. Commission Determination

23. We adopt the NOPR proposal to permit public utilities and non-public utilities that have or will have a rate on file with the Commission to seek incentive-based rate treatment for their eligible cybersecurity investments.[42]

24. We add § 35.48(a) to our regulations, which declares that the purpose of this section is to establish rules for incentive-based rate treatment for utilities with rates on file with the Commission that voluntarily make cybersecurity investments. In doing so, we adopt the NOPR proposal to allow utilities described in FPA section 201(f)[43] that have or will have a rate on file with the Commission to be eligible to receive incentives for cybersecurity investments in the same manner as public utilities. Accordingly, we add § 35.48(c) to our regulations, which states that the Commission will authorize incentive-based rate treatment to public and non-public utilities that have or will have a rate on file with the Commission for their voluntary cybersecurity investments, provided that the resulting rate is just and reasonable and not unduly discriminatory or preferential.

25. In FPA section 219A(c), Congress directs the Commission to offer incentive-based rate treatment for both the transmission of electric energy in interstate commerce and the sale of electric energy at wholesale in interstate commerce. This rulemaking satisfies the statutory requirement of providing the opportunity for public and non-public utilities to file to seek authorization to recover the cost of and receive incentive-based rate treatment on eligible cybersecurity investments.

26. We disagree with EPSA's contentions that utilities that make sales of energy, capacity, or ancillary services at market-based rates should be able to continue to make those sales and also separately recover the costs of, and receive incentive-based rate treatment on, eligible cybersecurity investments. The Incentive permitted in this final rule may only be recovered through a cost-of-service rate. As noted above, the ability to seek incentive-based rate treatment under this final rule meets the requirements of FPA section 219A.[44] All

[33] IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(c)).

[34] NOPR, 180 FERC ¶ 61,189 at P 1 n.3 (citing 16 U.S.C. 824s).

[35] APPA Initial Comments at 6.

[36] EPSA Initial Comments at 6–7.

[37] *Id.* at 6.

[38] *Id.* at 8.

[39] California Parties Reply Comments at 13.

[40] TAPS Initial Comments at 26–27.

[41] APPA Initial Comments at 22.

[42] NOPR, 180 FERC ¶ 61,189 at P 1 n.3.

[43] 16 U.S.C. 824(f).

[44] The dissent's criticism correctly notes that FPA section 219A is designed to provide incentives for certain cybersecurity investments. However, FPA section 219A also requires the Commission to

Continued

sellers of energy, capacity, and ancillary services are free to file cost-of-service rates under FPA section 205. Thus, we note that utilities currently making sales of energy, capacity, and ancillary services under market-based rate authority may make a filing to recover their entire cost of service, including costs of and an incentive on, eligible cybersecurity investments and proceed to make sales exclusively under that cost-based rate.[45]

2. Cybersecurity Investment Definitions

27. The cybersecurity investments eligible for incentives could include investments in Advanced Cybersecurity Technology, voluntary participation in a cybersecurity threat information sharing program, or both. Accordingly, we add § 35.48(b) to our regulations to define these and other terms used in that section. We incorporate the definitions of Advanced Cybersecurity Technology and Advanced Cybersecurity Technology Information in FPA section 219A(a).[46] Therefore, we define Advanced Cybersecurity Technology as 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 (as defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)).[47] We define Advanced Cybersecurity Technology Information as information relating to Advanced Cybersecurity Technology or proposed Advanced Cybersecurity Technology that is generated by or provided to the Commission or another Federal agency.[48] In accordance with FPA section 219A(g), Advanced Cybersecurity Technology Information is considered to be Critical Electric Infrastructure Information as that term is defined in FPA section 215A(a)(3) and § 388.113(c)(1) of the Commission's regulations.[49] We also define CEII in new subpart K as having the same meaning as that term is defined in § 388.113 of the Commission's regulations. In addition, we define Electric Reliability Organization and Reliability Standard as having the same meanings as those terms are defined in § 39.1 of the Commission's regulations.[50]

3. Cybersecurity Investment Eligibility Criteria

a. NOPR Proposal

28. In the NOPR, the Commission proposed that a cybersecurity investment must satisfy two eligibility criteria to be considered for a cybersecurity incentive.[51] First, the cybersecurity investment would need to materially improve cybersecurity through either an investment in Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program. Second, the cybersecurity investment could not already be mandated by CIP Reliability Standards, or otherwise mandated by local, State, or Federal law. Additionally, the Commission sought comment on whether, and if so how, the Commission should evaluate and ensure that the benefits of the cybersecurity investment exceed the combined costs of the cybersecurity investment and incentive, to ensure that the proposed rates are just and reasonable. The Commission also sought comment on whether these would be the appropriate criteria and whether there are additional criteria or limitations that the Commission 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).

29. The Commission proposed that, in determining which cybersecurity investments will materially improve a utility's security posture, the Commission will consider the following sources: (1) security controls enumerated in the NIST Special Publication (SP) 800–53 ''Security and Privacy Controls for Information Systems and Organizations'' catalog; [52] (2) security controls satisfying an objective found in the NIST Cybersecurity Framework; [53] (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); [54] (4) a specific recommendation from the CISA Shields Up Campaign; [55] (5) participation in the Cybersecurity Risk Information Sharing Program (CRISP) or similar cybersecurity threat information sharing program; and/or (6) the Cybersecurity Capability Maturity Model (C2M2) Domains [56] at the highest Maturity Indicator Level.[57] The Commission proposed that using these sources from 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 investments will be targeted and effective.

b. Comments

30. Microsoft Corporation (Microsoft) and the Michigan Public Service Commission (Michigan Commission) support the proposed eligibility criteria.[58] The Office of the Ohio Consumers' Counsel (Ohio Consumers' Counsel) also supports the proposed eligibility criteria and recommends that the Commission require utilities to demonstrate that their eligible expenditures provide quantifiable, incremental benefits to rate payers that will exceed expenditure cost.[59]

31. Alliant Energy Corporate Services, Inc. (Alliant), the Interstate Natural Gas Association of America (INGAA), the National Rural Electric Cooperative (NRECA), and APPA support the proposed eligibility criterion that a utility must show that a cybersecurity investment materially improves its cybersecurity posture for its investment to be eligible for an incentive.[60] While NRECA supports the proposed eligibility criterion, it is concerned that ''materially improves cybersecurity''

determine that any rate approved under this rule be just and reasonable, not unduly discriminatory or preferential. IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(e)). We agree with TAPS that the recovery of costs and an incentive as set forth in this final rule is not compatible with making sales at market-based rates. Therefore, our decision on this issue seeks to give meaning to all of the provisions of FPA section 219A.

[45] *Cf. PJM Interconnection, L.L.C.,* 178 FERC ¶ 61,121, at P 115 (2022) (noting generators' ability to choose between selling capacity at cost-based or market-based rates).

[46] IIJA, Public Law 117–58, section 40123, 135 Stat. 429, 951 (to be codified at 16 U.S.C. 824s–1(a)(1), (2)).

[47] *Id.* (to be codified at 16 U.S.C. 824s–1(a)(1)).

[48] *Id.* (to be codified at 16 U.S.C. 824s–1(a)(2)).

[49] 16 U.S.C. 824o–1(a)(3); 18 CFR 388.113(c)(1).

[50] 18 CFR 39.1.

[51] NOPR, 180 FERC ¶ 61,189 at P 20.

[52] 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.*

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

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

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

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

[57] NOPR, 180 FERC ¶ 61,189 at P 21.

[58] Microsoft Initial Comments at 1; Michigan Commission Initial Comments at 5–6.

[59] Ohio Consumers' Counsel Initial Comments at 4–5.

[60] Alliant Initial Comments at 3–4; INGAA Initial Comments at 3; NRECA Initial Comments at 4–5; APPA Initial Comments at 3.

may be too subjective to ensure that cybersecurity investments provide adequate benefits to customers.[61] NRECA recommends that the Commission specify additional criteria or establish a minimum level of benefit or value a cybersecurity investment would provide to be eligible.[62]

32. The Public Utilities Commission of Ohio's Office of the Federal Energy Advocate (Ohio FEA) and Edison Electric Institute (EEI) do not support the proposed eligibility criterion that a cybersecurity investment must materially improve cybersecurity.[63] Ohio FEA asserts that the term ''materially improves'' may be ambiguous and suggests that the Commission should provide additional detail regarding this criterion in order to achieve its objective and streamline review of cybersecurity incentives.[64] EEI argues that applying a ''materially improve'' test will lead to subjective and inconsistent results because it is unclear what additional insights the Commission would reference beyond the six sources from other agencies to satisfy the criterion.[65] EEI argues that the materiality test is not part of the statutory language and will not necessarily improve the cybersecurity posture of the filing utility.[66] EEI recommends that, instead, the Commission give utilities the flexibility to propose other sources than the six listed in the NOPR and provide context for why a cybersecurity investment supports a targeted level of cyber maturity within a broader cybersecurity risk management and control framework.[67]

33. Ohio FEA supports the Commission referencing other Federal agencies and activities to determine whether a cybersecurity investment materially improves cybersecurity but asserts that the final determination should be based on the specific circumstances of the filing utility.[68] INGAA recommends that the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) be added to the sources used to inform the Commission's determination of whether a particular cybersecurity investment satisfies the first eligibility criterion.[69] DOE states that, while the six sources listed in the NOPR are beneficial and valuable, they are not a comprehensive list of ways that cybersecurity can be measured.[70] SecurityScorecard recommends that international standards such as ISO/IEC 27000 and Information Systems Audit and Control Association's Control Objectives for Information and Related Technologies also be considered when assessing the materiality criteria.[71]

34. DOE and EEI recommend that the Commission adjust the eligibility criteria referencing the C2M2 Domains from the highest Maturity Indicator Level to lower, incremental levels.[72] DOE and EEI argue that investments made to reach lower, incremental maturity levels would be more valuable than overinvestment in unnecessary controls to reach the highest Maturity Indicator Level.[73]

35. Most commenters support the idea that expenditures already mandated by local, State, or Federal law or an enforceable CIP Reliability Standard should not be eligible for an incentive. EEI, NRECA, and INGAA support this eligibility criterion as proposed in the NOPR. Other commenters argue that the proposed criterion should be expanded to include other types of legally binding agreements or Reliability Standards.[74] TAPS, APPA, Ohio FEA, California Parties, and the Maryland Public Service Commission and Pennsylvania Public Utility Commission (Maryland and Pennsylvania Commissions) argue that investments made to satisfy any type of legal obligation should be ineligible for an incentive, including, for example, remedial measures as a settlement of NERC compliance violations, a condition of a State or Federal license, a condition of a merger proceeding, and an obligation under a cybersecurity insurance policy.[75] APPA further recommends that the Commission clarify whether investments are ineligible if mandated by only CIP Reliability Standards or also by any other mandatory Reliability Standard.[76] In addition to an expanded definition of ''mandated,'' TAPS recommends that the Commission require a filing utility to attest that a cybersecurity investment for which it seeks incentives is not being made to satisfy any legal obligation.[77]

36. The North American Electric Reliability Corporation and the six Regional Entities[78] (NERC) states that any voluntary incentives should build upon and complement existing cybersecurity CIP Reliability Standards.[79] NERC recommends that the Commission consider the relationship between voluntary cybersecurity investments and mandatory CIP Reliability Standards and cautions that it may be a challenge for the Commission to determine whether a particular investment is mandated by the CIP Reliability Standards.[80] NERC explains that, because the CIP Reliability Standards are outcome oriented and do not prescribe specific technologies, a utility may file for an incentive that, while not mandated, is being used to comply with mandatory CIP Reliability Standards.[81] TAPS similarly states that the Commission should take a nuanced approach to assess whether a technology exceeds the CIP Reliability Standards when a technology has been used to comply with, but is not specifically mandated by, a CIP Reliability Standard.[82] NRECA urges the Commission to consider whether it will grant incentives for cybersecurity expenditures that enhance the cybersecurity of low impact BES Cyber Systems or only medium or high impact BES Cyber Systems.[83]

37. California Parties support the addition of an eligibility criterion for information-sharing programs that the incentives be conditioned on utilities participating in all applicable regional and State cybersecurity initiatives.[84] DOE recommends that the Commission establish attributes that the Commission will consider when determining the eligibility of information-sharing programs for incentives.[85]

c. Commission Determination

38. We adopt and modify the NOPR proposal by adding § 35.48(d) to the Commission's regulations to permit a utility to receive incentive-based rate

[61] NRECA Initial Comments at 4–5.

[62] *Id.* at 5.

[63] EEI Initial Comments at 8; Ohio FEA Initial Comments at 5–6.

[64] Ohio FEA Initial Comments at 5–6.

[65] EEI Initial Comments at 8.

[66] *Id.* at 8.

[67] *Id.* at 8.

[68] Ohio FEA Initial Comments at 5–6.

[69] INGAA Initial Comments at 3.

[70] DOE Reply Comments at 6.

[71] SecurityScorecard Initial Comments at 4.

[72] DOE Reply Comments at 8–9; EEI Initial Comments at 8–9.

[73] DOE Reply Comments at 8; EEI Initial Comments at 8.

[74] TAPS Initial Comments at 9–12; APPA Initial Comments at 13; Ohio FEA Initial Comments at 6; California Parties Initial Comments at 20; Maryland and Pennsylvania Commissions Initial Comments at 8.

[75] TAPS Initial Comments at 12.

[76] APPA Initial Comments at 13.

[77] TAPS Initial Comments at 12.

[78] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

[79] NERC Initial Comments at 3.

[80] *Id.* at 4.

[81] *Id.* at 4–5.

[82] TAPS Initial Comments at 12.

[83] NRECA Initial Comments at 5; *see* NERC Glossary defining BES Cyber Systems.

[84] California Parties Initial Comments at 5.

[85] DOE Reply Comments at 10.

treatment for a cybersecurity investment. We establish two eligibility criteria that require that each cybersecurity investment: (1) materially improves cybersecurity through either Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program; and (2) is not already mandated by the Reliability Standards, or otherwise mandated by local, State, or Federal law, decision, or directive; otherwise legally mandated; or an action taken in response to a Federal or State agency merger condition, consent decree from Federal or State agency, or settlement agreement that resolves a dispute between a utility and a public or private party.[86]

39. In the NOPR, the Commission identified several sources that the Commission would consider as part of its evaluation of whether a cybersecurity investment would materially improve a utility's security posture, thereby providing quantifiable cybersecurity benefits.[87] Based on the comments received, we modify the NOPR proposal.

40. As recommended by INGAA, we find that the Commission should also consider specific recommendations from the FBI and NSA. Therefore, we find that, in determining which cybersecurity investments 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; [88] (2) security controls satisfying an objective found in the NIST Cybersecurity Framework [89] technical subcategory; (3) a specific cybersecurity recommendation from a relevant Federal authority, such as DHS's CISA, the FBI, NSA, or DOE; [90] (4) participation in a relevant cybersecurity threat information sharing program; and/or (5) achieving and sustaining one or more of the C2M2 Domains at the highest Maturity Indicator Level.[91] Considering these sources as part of a Commission determination of whether a particular cybersecurity investment would materially improve cybersecurity will allow the Commission to approve objective, targeted, and effective cybersecurity investments for incentive treatment.[92]

41. In addition, we agree with DOE's and Ohio FEA's recommendation that the Commission expand the list of potential eligible cybersecurity threat information sharing programs beyond CRISP. We clarify that a utility may seek an incentive for participation in other cybersecurity threat information sharing programs and the Commission will consider whether such cybersecurity threat information sharing programs would qualify for incentive treatment. We will not, as EEI suggests, consider recommendations other than the five sources described above. Considering other sources would increase subjectivity and unpredictability of incentive-based rate treatment of cybersecurity investments.

42. We agree with DOE's and California Parties' recommendation that the Commission should establish eligibility criteria or attributes in evaluating cybersecurity threat information-sharing programs. The Commission will evaluate any proposed relevant cybersecurity threat information-sharing program to determine whether the program: (1) is sponsored by the Federal or State government; (2) provides two-way communications from and to electric industry and government entities; and (3) delivers relevant and actionable cybersecurity information to program participants from the United States electricity industry.

43. We decline to adopt SecurityScorecard's recommendation that the Commission consider international standards, such as ISO/IEC 27000, when assessing the materiality criteria. Like NIST SP 800–53, ISO/IEC 27000 provides a catalog of information and cyber-related security controls. While there are some differences in focus between the two standards, for the context of determining how to successfully categorize a cybersecurity investment used to improve the security posture of a utility, both standards perform similar functions. Therefore, we believe that considering such international standards in assessing materiality would be duplicative and unnecessary and we will not adopt this recommendation. Instead, we will use NIST SP 800–53 as the foundation of security controls to evaluate whether a cybersecurity investment materially improves the cybersecurity of a utility because NIST SP 800–53 was developed by a Federal agency and is publicly accessible without additional cost.

44. We also decline to adopt DOE and EEI's recommendation that the Commission provide incentives for any incremental steps taken by utilities in connection with C2M2 and not just for achieving the highest Maturity Indicator Level. The C2M2 model contains descriptive cybersecurity measures at a high level rather than prescriptive requirements. Therefore, it would be difficult for the Commission to determine that compliance with incremental steps necessarily materially improves cybersecurity. For these reasons, we are requiring a utility to demonstrate that its proposed cybersecurity investments will cause the utility to achieve Maturity Indicator Level 3 of the C2M2 Domains rather than the incremental steps of the lower Maturity Indicator Levels in order to receive an incentive for its cybersecurity investments.

45. TAPS, APPA, Ohio FEA, California Parties, and the Maryland and Pennsylvania Commissions request that the Commission ensure that investments made to satisfy any type of legal obligation be ineligible for an incentive. The Maryland and Pennsylvania

[86] As the dissent points out, FPA section 219A(c) directs the Commission to establish rate incentives for participation by public utilities in cybersecurity threat information sharing programs and investments by public utilities in Advanced Cybersecurity Technology, which it defines as 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 cyber security threat. Public Law 117–58, section 40123(a), 135 Stat. 429, 951 (codified 16 U.S.C. 824s–1(c)). FPA section 219A also specifies that such rate treatments exist for the purpose of benefitting consumers and requires that the Commission ensure that resulting rates be just and reasonable. *See* Public Law 117–58, section 40123(a), 135 Stat. 429, 951 (codified 16 U.S.C. 824s–1(a) & (c)). The materially improves incentive eligibility criterion seeks to balance these statutory requirements. Solely focusing on the term enhance may result in the Commission granting incentives that do not meet these other statutory requirements mentioned above. It is thus reasonable for the Commission to exercise its judgement via the materially improves eligibility criterion to evaluate incentives requests.

[87] In section III.B., we discuss different methods that utilities could use to show how their cybersecurity investments satisfy the eligibility criteria.

[88] 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.*

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

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

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

[92] As we discuss in section III.B.1., when considering whether to add a cybersecurity investment to the PQ List, the Commission will determine whether the cybersecurity investment would materially improve cybersecurity for all utilities. As we discuss in section III.B.2., when evaluating a utility case-by-case application for incentive-based rate treatment for a particular cybersecurity investment, the Commission will determine whether the cybersecurity investment would materially improve cybersecurity for the utility requesting the incentive-based rate treatment.

Commissions comment that utilities should not receive incentives for implementing cybersecurity measures that are already made mandatory by existing and future obligations.[93] APPA comments that the Commission should broaden the second eligibility criterion to clarify that incentives would not be available for cybersecurity investments for mandatory Reliability Standards and that the Commission should replace the reference to the CIP Reliability Standards with Reliability Standards.[94] We agree with both suggestions. Accordingly, we are expanding the second eligibility criterion to emphasize the requirement that the utility must undertake the specific cybersecurity investment voluntarily in order to receive a cybersecurity incentive pursuant to our regulations. Our revised § 35.48(d)(2) provides that a cybersecurity investment is only eligible for an incentive if it is not already mandated by the Reliability Standards as maintained by the Electric Reliability Organization, or otherwise mandated by local, State, or Federal law, decision, or directive; otherwise legally mandated; or an action taken in response to a Federal or State agency merger condition, consent decree from Federal or State agency, or settlement agreement that resolves a dispute between a utility and a public or private party.[95]

46. Additionally, we recognize the concerns raised by NERC and TAPS about the difficulty in determining whether a particular cybersecurity investment is mandatory. Accordingly, as discussed in greater detail in section III.D.3., we are adopting TAPS's suggestion that, in order to demonstrate that the specific cybersecurity investment for which the utility is seeking an incentive is voluntary, the applicant must include an attestation in its filing so stating.[96]

47. TAPS raises issues about technologies that both meet and exceed the Reliability Standards. We recognize that there could be a single Advanced Cybersecurity Technology that provides multiple security controls that allow the utility to meet and potentially exceed compliance with a Reliability Standard. In that instance, where the utility makes a single cybersecurity investment for security controls to comply with a Reliability Standard, that investment will not be incentive-eligible. However, there may be instances where a utility invests in a single Advanced Cybersecurity Technology that while complying with a Reliability Standard also provides enhanced cybersecurity controls that go beyond compliance with a Requirement in the Reliability Standard. In those instances, only the incremental investment to exceed the Requirement of the Reliability Standard would be eligible for an incentive.

48. In response to NRECA's concerns regarding the reliability and security of low impact BES Cyber Systems, we are not requiring any eligibility criteria other than the two discussed above. Therefore, low impact BES Cyber Systems are not excluded from eligibility for incentive-based rate treatment for cybersecurity investments.

49. We disagree with EEI's conclusion that we should omit ''materially improve'' as the standard for the first eligibility criterion due to its absence from the statutory language and possible subjectivity. FPA section 219A requires the Commission to offer incentives for Advanced Cybersecurity Technology investments and participation in information-sharing programs. It does not require that the Commission provide incentives for *all* Advanced Cybersecurity Investments or participation in *any* information-sharing program. FPA section 219A also requires that the Commission ensure that rates are just and reasonable and not unduly discriminatory or preferential.[97] Without a materiality standard in the first criterion (or something similar), any Advanced Cybersecurity Investment that is not mandatory would be incentive-eligible, regardless of whether such investments enhance a utility's security posture or result in just and reasonable rates. Furthermore, use of such a standard is consistent with Commission precedent. In Order No. 679, the Commission required applicants for transmission incentives to show that requested incentives are tailored to the risks and challenges of individual projects, even though such a requirement is not included in the statutory language of FPA section 219.[98]

50. We recognize that the materially improves criterion requires use of Commission subject matter expertise and judgement. In exercising its subject matter expertise and judgement, the Commission will take into account the findings of other Federal agencies to inform its decisions, as described in section III.B.2.c. Although the Commission seeks to maximize predictability and transparency in its provision of incentives, some degree of judgement is necessary given the many types of cybersecurity threats and investments and their rapid evolution. It is for this reason that we also decline NRECA's request that the Commission provide additional criteria or a baseline level of benefit. As discussed in section III.C.3., quantification of benefits may be difficult for cybersecurity investments, such that a bright line benefit requirement is inappropriate. In this final rule, we are establishing eligibility criteria that balance the need to ensure that incentives are targeted at the most beneficial investments with recognizing that there are many potential cybersecurity investments which could provide a wide variety of benefits. We find that overly prescriptive eligibility criteria may unduly preclude incentive-based rate treatment of beneficial cybersecurity investments.

51. Although the Commission sought comment on whether, and if so how, the Commission should evaluate and ensure that the benefits of the cybersecurity investment exceed the combined costs of the cybersecurity investment and the incentive, to ensure that the proposed rates are just and reasonable, we will not at this time predicate incentive eligibility on such a cost-benefit showing. As the Commission proposed in the NOPR and we affirm here, the rates, including the costs of any incentive, must remain within the zone of reasonableness. This is necessary to ensure that the rates that include incentives for cybersecurity investments are just and reasonable and not unduly discriminatory or preferential.

52. Ohio Consumers' Counsel argues that there must be quantifiable, incremental benefits that can be measured in cost-benefit savings to consumers. Nevertheless, we find that quantification of the costs and benefits for each cybersecurity investment is

[93] Maryland and Pennsylvania Commissions Initial Comments at 8.

[94] APPA Initial Comments at 5.

[95] A mandate must either be for a utility to achieve a specific outcome or to require a utility to take a prescribed action. General mandates to improve a utility's cybersecurity may still make specific cybersecurity investments voluntary for purposes of the Commission's evaluation of the eligibility criteria.

[96] The attestation must be made by a senior person within the utility that the utility has authorized to act on behalf of the utility. One example of a senior person could be the CIP Senior Manager as NERC defines that term. NERC Glossary at 10 (defining CIP Senior Manager to mean ''A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP–002 through CIP–011.'').

[97] FPA section 219A(e)(1). FPA section 219A(e)(2) also prohibits unjust and unreasonable double recovery for Advanced Cybersecurity Technology. IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(e)(2)).

[98] *See Promoting Transmission Investment Through Pricing Reform,* Order No. 679, 71 FR 43294 (July 31, 2006), 116 FERC ¶ 61,057, at P 26, *order on reh'g,* Order No. 679–A, 72 FR 1152 (Jan. 10, 2007), 117 FERC ¶ 61,345 (2006), *order on reh'g,* 119 FERC ¶ 61,062 (2007).

neither required nor practical. Such a cost-benefit analysis is particularly inapt for cybersecurity where benefits are even harder to identify and quantify than are economic and reliability benefits for transmission investments. The courts have long recognized that a primary purpose of the FPA, and its counterpart the Natural Gas Act (NGA), is to encourage the orderly development of plentiful supplies of electricity and natural gas at reasonable prices.[99] To carry out this purpose, the Commission may consider non-cost factors as well as cost factors.[100] Moreover, Congress' enactment of section 219A reflects its determination that incentives generally can spur cybersecurity investments and their associated consumer benefits.

53. As the Commission proposed in the NOPR, we find that all cybersecurity investments must satisfy both of the eligibility criteria in order to be eligible for incentive treatment. In addition, we now clarify that a utility may not request an incentive for a cybersecurity investment that the utility has already been incurring for more than three months prior to the filing of the incentive application, as discussed in section III.C.2 of this final rule, unless that cybersecurity investment is for participation in an incentive-eligible cybersecurity threat information sharing program.

B. Cybersecurity Investment Incentive Requests

54. In order to maximize predictability and transparency in our provision of incentives, we provide below a framework for evaluating whether certain cybersecurity investments, including expenses and capitalized costs, are eligible for a cybersecurity incentive. First, as the Commission proposed in the NOPR, we include a list of pre-qualified investments, the PQ List, to identify certain cybersecurity investments that the Commission finds merit the rebuttable presumption of eligibility for all utilities and are therefore eligible for incentive-based rate treatment. We also discuss the procedures that we will use to update the PQ List. Second, we adopt the cybersecurity investments proposed in the NOPR for inclusion on the initial PQ List. Third, we describe how the Commission will evaluate whether a utility's cybersecurity investments that are not included on the PQ List may be eligible for incentive-based rate treatment. Finally, we discuss how a utility can seek incentive-based rate treatment for new cybersecurity investments made to comply with a Reliability Standard during the period after the Commission approves a new or modified cybersecurity Reliability Standard but before that new or modified cybersecurity Reliability Standard becomes mandatory and enforceable.

1. PQ List Approach

a. Structure of the PQ List

i. NOPR Proposal

55. In the NOPR, the Commission proposed to create a PQ List that would identify cybersecurity investments that the Commission determined would satisfy the eligibility criteria.[101] The Commission proposed that any cybersecurity investment that the Commission includes on the PQ List would be entitled to a rebuttable presumption of eligibility for an incentive.[102] However, an applicant would still need to demonstrate, and the Commission would need to find, that the proposed rate, inclusive of the cybersecurity incentive, is just and reasonable. The Commission proposed to provide an opportunity for protestors to rebut this presumption by demonstrating that the cybersecurity investment did 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 based on other evidence.

56. The Commission explained that the PQ List approach would provide efficiency and transparency benefits.[103] The utility-specific incentive filings under the PQ List approach could be substantially streamlined compared to a case-by-case approach because the Commission would have pre-reviewed the cybersecurity investments included on the PQ List for eligibility for incentives.

57. In the NOPR, the Commission noted the rapidly evolving nature of cybersecurity threats and solutions and that it expected to regularly evaluate the PQ List and update it as necessary.[104] When updating the PQ List, the Commission could add, modify, or remove cybersecurity investments to/from the PQ List. The Commission proposed that it would update the PQ List via a rulemaking, whether *sua sponte* or in response to a petition.

ii. Comments

58. INGAA, Microsoft, TAPS, the Michigan Commission, Ohio Consumers' Counsel, ITC Companies, APPA, Anterix, Inc. (Anterix), OT Coalition, Avangrid, Inc. (Avangrid), MISO Transmission Owners, EPSA, and EEI support the PQ List approach.[105] OT Coalition, Avangrid, MISO Transmission Owners, EPSA, and EEI further urge the Commission to consider using both the PQ List and case-by-case approaches.[106] ITC Companies agree with the Commission that the PQ List approach will decrease the filing and review burden on utilities and the Commission [107] while INGAA and Microsoft agree that the PQ List approach will provide transparency for utilities as to what expenditures will be eligible for incentives.[108] Microsoft and Anterix caveat their support of the PQ List approach by suggesting other items for inclusion on the PQ List, such as security incident and event monitoring, user and entity behavior analysis,[109] and private LTE wireless broadband communication systems.[110] TAPS, Michigan Commission, and Ohio Consumers' Counsel recommend that the PQ List be updated regularly,[111] and APPA underscores the need for stakeholders to have the opportunity to rebut the presumption of eligibility.[112]

59. In contrast, Alliant, the Maryland and Pennsylvania Commissions, and DOE assert that that the PQ List approach with its rebuttable presumption of eligibility will lessen innovation by encouraging utilities to pursue the same types of cybersecurity investments (*i.e.,* those on the PQ List), regardless of the utility's individual

[99] Order No. 679, 116 FERC ¶ 61,057 at P 65 (citing *Pub. Util. Comm'n of the State of Cal.* v. *FERC,* 367 F.3d 925, 929 (D.C. Cir. 2004) (citing *NAACP* v. *FPC,* 425 U.S. 662, 670 (1976))).

[100] *Id.* (citing *Permian Basin Area Rate Cases,* 390 U.S. 747, 791, 815 (1968); *Me. Pub. Utils. Comm'n* v. *FERC,* 454 F.3d 278, 288 (DC Cir. 2006)).

[101] NOPR, 180 FERC ¶ 61,189 at P 25.

[102] *Id.* P 26.

[103] *Id.* P 27.

[104] *Id.* P 31.

[105] INGAA Initial Comments at 4; Microsoft Initial Comments at 2; TAPS Initial Comments at 4; Michigan Commission Initial Comments at 6; Ohio Consumers' Counsel Initial Comments at 8–9; ITC Companies Initial Comments at 4–5; APPA Initial Comments at 17; Anterix Initial Comments at 5; OT Coalition Initial Comments at 2; Avangrid Initial Comments at 5; MISO Transmission Owners Initial Comments at 6–7; EPSA Initial Comments at 5; EEI Initial Comments at 5.

[106] OT Coalition Initial Comments at 2; Avangrid Initial Comments at 5; MISO Transmission Owners Initial Comments at 6–7; EPSA Initial Comments at 5; EEI Comments at 5.

[107] ITC Companies Initial Comments at 4–5.

[108] INGAA Initial Comments at 4; Microsoft Initial Comments at 2.

[109] Microsoft Initial Comments at 1–2.

[110] Anterix Initial Comments at 5.

[111] TAPS Initial Comments at 6; Michigan Commission Initial Comments at 6; Ohio Consumers' Counsel Initial Comments at 8–9.

[112] APPA Initial Comments at 5.

needs and risks.[113] California Parties, while not necessarily opposed to the concept of a PQ List approach, strongly oppose giving filing utilities a rebuttable presumption of eligibility for expenditures on the PQ List.[114] They argue that the burden on a party seeking to rebut the presumption of eligibility is too great.[115]

60. Many commenters raise concerns that finding a balance between transparency and security will prove challenging for the Commission. NRECA cautions that a publicly accessible PQ List will alert adversaries to the cybersecurity activities of utilities and create a security risk.[116] Alliant recommends that, if the Commission decides to proceed with the PQ List approach, it defer to NERC for identification of technologies and designate the PQ List as CEII to protect it from public access.[117] On the other hand, California Parties and the Maryland and Pennsylvania Commissions underscore the need for public transparency and access to allow stakeholders to rebut the presumption of eligibility and utilities to know what types of expenditures are eligible.[118]

61. Some commenters describe the challenges that maintaining an updated PQ List will present for the Commission. Ohio FEA and the Maryland and Pennsylvania Commissions express concern that the Commission may be unable to maintain a current PQ List, due to the lengthy regulatory process required,[119] potentially leading to overinvestment in outdated measures and underinvestment in cutting edge technologies.[120] Most commenters support frequent and regular review and updates to the PQ List.[121] EEI recommends that the Commission commit to reviewing and updating the PQ List on a regular cadence no less than annually, while Anterix, Avangrid, TAPS, and Ohio Consumers' Counsel suggest regular and expeditious updates.[122] TAPS and Ohio Consumers' Counsel recommend that, when the Commission initiates a rulemaking to modify the PQ List, it should assess whether existing expenditures still meet the eligibility criteria in addition to assessing new additions.[123]

62. California Parties and NRECA emphasize that modifications to the PQ List should only be made via a full rulemaking process where stakeholders and customers have the opportunity to comment.[124] California Parties further argue that the Commission should not expand the initial PQ List in its final rule without a full notice-and-comment period for the suggested additions.[125] TAPS highlights that the rulemaking process will improve regulatory certainty for utilities and customers and facilitate participation and input on whether proposed expenditures meet the eligibility criteria.[126]

63. Indicated PJM Transmission Owners [127] and Anterix recommend that the Commission hold a technical conference to inform its decision making on reviewing and updating the eligible expenditures on the PQ List.[128]

iii. Commission Determination

64. We adopt and modify the NOPR's proposal to create a PQ List by adding § 35.48(e)(1) to the Commission's regulations, which establishes the framework for a PQ List of cybersecurity investments that the Commission finds materially improves cybersecurity. We find that the cybersecurity investments on the PQ List would be entitled to a presumption of satisfying the eligibility criteria. As proposed in the NOPR, protestors may seek to rebut this presumption by demonstrating that, given the unique circumstances of the utility, the cybersecurity investment on the PQ List would not materially improve cybersecurity of the utility. We note that the utility would still need to demonstrate that it would make the cybersecurity investment voluntarily. In addition, the Commission will not presume anything about the resulting rates. Utilities seeking an incentive under the PQ List must still show that the proposed rate, including the cybersecurity incentive, is just and reasonable and not unduly discriminatory or preferential.

65. The PQ List approach is also in line with FPA section 219A(d)(2), which allows the Commission to reduce the cybersecurity risks to the facilities of small or medium-sized public utilities with limited cybersecurity resources.[129] While all utilities would benefit from the reduced filing obligations when requesting incentive treatment for cybersecurity investments on the PQ List, we expect that this approach would be particularly beneficial for small and medium-sized utilities with limited cybersecurity resources.

66. We disagree with concerns that including cybersecurity investments on the PQ List would lessen cybersecurity innovation or alert adversaries of utility cybersecurity investment. Regarding lessening innovation, as an initial matter, we note that utilities may still seek to recover in their rates all prudently incurred cybersecurity investments. Furthermore, as described in section III.B.2, we are adding a case-by-case approach that may better incent cybersecurity investments responding to rapidly evolving threats than does the PQ List. Regarding concerns about alerting adversaries, we find that such assertions are speculative and that describing and providing incentives to broadly beneficial cybersecurity investments will not unto itself

[113] Alliant Initial Comments at 4–5; Maryland and Pennsylvania Commissions Initial Comments at 6.

[114] California Parties Initial Comments at 28–29.

[115] *Id.;* California Parties Reply Comments at 11–12.

[116] NRECA Initial Comments at 7–8.

[117] Alliant Initial Comments at 4–5.

[118] California Parties Initial Comments at 28–29; Maryland and Pennsylvania Commissions Initial Comments at 5–6.

[119] Ohio FEA Initial Comments at 14; Maryland and Pennsylvania Commissions Initial Comments at 5.

[120] Maryland and Pennsylvania Commissions Initial Comments at 5.

[121] Avangrid Initial Comments at 5; EEI Initial Comments at 6–7; TAPS Initial Comments at 5; Ohio Consumers' Counsel Initial Comments at 8; Anterix Reply Comments at 4.

[122] EEI Initial Comments at 6–7; Anterix Reply Comments at 4.; Avangrid Initial Comments at 5; TAPS Initial Comments at 5; Ohio Consumers' Counsel Initial Comments at 7.

[123] TAPS Initial Comments at 5; Ohio Consumers' Counsel Initial Comments at 8.

[124] NRECA Initial Comments at 8–9; California Parties Initial Comments at 33–34.

[125] California Parties Initial Comments at 11–12.

[126] TAPS Initial Comments at 5.

[127] Indicated PJM Transmission Owners consist of: American Electric Power Service Corporation on behalf of its affiliates, Appalachian Power Company, Indiana Michigan Power Company, Kentucky Power Company, Kingsport Power Company, Ohio Power Company, Wheeling Power Company, AEP Appalachian Transmission Company, Inc., AEP Indiana Michigan Transmission Company, Inc., AEP Kentucky Transmission Company, Inc., AEP Ohio Transmission Company, Inc., and AEP West Virginia Transmission Company, Inc.; Dayton Power and Light Company d/b/a AES Ohio; Dominion Energy Services, Inc. on behalf of Virginia Electric and Power Company d/b/a Dominion Energy Virginia; Duke Energy Corporation on behalf of its affiliates Duke Energy Ohio, Inc., Duke Energy Kentucky, Inc., and Duke Energy Business Services LLC; Duquesne Light Company; East Kentucky Power Cooperative; Exelon Corporation; FirstEnergy Service Company, on behalf of its affiliates American Transmission Systems, Incorporated, Jersey Central Power & Light Company, Mid-Monongahela Power Company, Keystone Appalachian Transmission Company, and Trans-Allegheny Interstate Line Company; PPL Electric Utilities Corporation; Public Service Electric and Gas Company; Rockland Electric Company; and UGI Utilities Inc.

[128] Indicated PJM Transmission Owners Initial Comments at 5; Anterix Initial Comments at 12–13.

[129] FPA section 219A(d)(2) provides that the Commission may provide additional incentives beyond incentive-based rate treatment in any case which the Commission determines that an investment in Advanced Cybersecurity Technology or in information sharing program costs will reduce cybersecurity risks to facilities of small or medium-sized public utilities with limited cybersecurity resources, as determined by the Commission. IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(d)(2)).

highlight either industry-wide or utility-specific vulnerabilities.

67. We disagree with comments recommending that we designate the PQ List as CEII. The PQ List does not meet the definition of CEII, because the list is general in nature and does not reveal specific vulnerabilities.[130] As discussed in section III.D.3.c., requests for incentive-based rate treatment for cybersecurity investments may include requests for CEII treatment consistent with our regulations.[131] As we approve additional PQ List items, we expect that any future PQ List item will not be more specific than what can be found in the already publicly available materials, such as the NIST publications and CIP Reliability Standards. We decline to adopt Alliant's recommendation that the Commission defer to NERC to identify eligible technologies for the PQ List. The Commission will evaluate potential cybersecurity technologies from time to time, and determine, based on the record evidence, whether it would be appropriate to add the proposed cybersecurity investments in these technologies to the PQ List.

68. We disagree with comments that the PQ List approach places an undue burden on parties seeking to rebut the presumption of eligibility. We believe that the PQ List approach appropriately balances the interests of the utilities and any potential protestors seeking to rebut the presumption of eligibility. By starting with the initial PQ List, we have identified specific cybersecurity investments that we find will materially improve the cybersecurity of utilities broadly, while enabling protestors to demonstrate that the eligibility criteria are not met in a utility's particular circumstance.

69. We acknowledge the concerns raised by commenters regarding the time necessary for the Commission to modify the PQ List. Some commenters request that the Commission commit to a regular update cycle for the PQ List. In this final rule, the Commission modifies the proposed regulation to allow the Commission to post the PQ List on its website and to update it subject to a notice and comment period or in a rulemaking. In addition, the case-by-case approach allows the Commission to evaluate whether a utility's cybersecurity investment would satisfy the eligibility criteria as to that utility. This means that utilities would not have to wait for the Commission to update the PQ List before seeking incentives for cybersecurity investments not yet included on the PQ List. In response to Indicated PJM Transmission Owners and Anterix's suggestion to have a technical conference when considering updates to the PQ List, we note that the Commission will consider such action when undertaking its periodic PQ List reviews.

b. Initial PQ Lis

i. NOPR Proposal

70. The Commission proposed to include two eligible cybersecurity investments on the initial PQ List: (1) expenditures associated with participation in CRISP;[132] and (2) expenditures associated with internal network security monitoring within the utility's cyber systems, which could include IT cyber systems and/or OT cyber systems, and which could be associated with cyber systems that may or may not be subject to the Reliability Standards.[133] The Commission believed that these cybersecurity investments would materially improve cybersecurity[134] and were not already mandated by the Reliability Standards[135] or otherwise mandated by Federal law. The Commission proposed to include CRISP, as its purpose is to facilitate the timely bi-directional sharing of unclassified and classified threat information and development of situational awareness tools that enhance the energy sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.[136]

71. The Commission also proposed to include internal network security monitoring on the PQ List because internal network security monitoring may better position a utility to detect malicious activity that has circumvented perimeter controls.[137] The Commission observed that, while the currently effective Reliability Standards do not require internal network security monitoring, NERC has recognized the proliferation and usefulness of such technology.[138] The Commission also sought comments on whether to include any additional cybersecurity investments on the initial PQ List.

ii. Comments

72. NERC, DOE, and Microsoft support the inclusion of CRISP on the PQ List.[139] EEI and American Electric Power Service Corporation (AEP) support incentives for both new and existing participants of CRISP.[140] EEI argues that, because participation in cybersecurity threat information sharing programs is an ongoing action and CRISP participants have to occasionally upgrade technology, existing participants should be eligible to receive an incentive.[141]

73. APPA and California Parties oppose the Commission providing incentives for existing CRISP participants.[142] APPA and California Parties argue that an incentive must be an inducement for future action and cannot provide an incentive for actions already taken, such as recovery of an incentive for ongoing participation in CRISP if a utility is already a participant.[143] APPA further adds that CRISP participants report high satisfaction with the program and thus do not need an incentive to continue participation.[144] The Maryland and Pennsylvania Commissions and California Parties note that most major

[130] *See* 18 CFR 388.113(c).

[131] *See* 18 CFR 388.113.

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

[133] NOPR, 180 FERC ¶ 61,189 at P 28.

[134] 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.

[135] The Commission noted in the NOPR that it had already proposed to require NERC to develop and submit for Commission approval a mandatory Reliability Standard regarding internal network analysis and monitoring technologies for high and medium impact bulk electric system cyber systems. *See* NOPR, 180 FERC ¶ 61,189 at P 28 n.26 (citing *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Syss.,* Notice of Proposed Rulemaking, 87 FR 4173 (Jan. 27, 2022), 178 FERC ¶ 61,038 (2022)). The Commission has since issued a final rule directing NERC to develop and submit for Commission approval a Reliability Standard that addresses internal network security monitoring for high impact bulk electric system cyber systems and medium impact bulk electric system cyber systems with external routable connectivity. *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Syss.,* Order No. 887, 88 FR 8354 (Feb. 9, 2023), 182 FERC ¶ 61,021 (2023).

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

[137] NOPR, 180 FERC ¶ 61,189 at P 29.

[138] *Id.* (citing NERC, *ERO Enterprise CMEP Practice Guide: Network Monitoring Sensors, Centralized Collectors, and Information Sharing,* 1 (June 4, 2021), *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 DOE initiative ''to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for [industrial control systems] of electric utilities.'').

[139] NERC Initial Comments at 3; DOE Reply Comments at 7; Microsoft Initial Comments at 2.

[140] EEI Initial Comments at 11; EEI Reply Comments at 5. AEP Initial Comments at 4.

[141] EEI Initial Comments at 11; EEI Reply Comments at 5.

[142] APPA Initial Comments at 5; California Parties Initial Comments at 10; California Parties Reply Comments at 8–9.

[143] APPA Initial Comments at 12–13; California Parties Initial Comments at 10; California Parties Reply Comments at 8–9.

[144] APPA Initial Comments at 13–14.

investor-owned utilities are already part of CRISP, whether individually or as members of a respective regional transmission organization or independent system operator.[145]

74. EEI, UMass Lowell Applied Research Corporation (UMLARC), Ohio FEA, and Microsoft recommend that the Commission consider for inclusion on the PQ List additional eligible cybersecurity threat information sharing programs.[146] EEI recommends that the PQ List be expanded to include other federally funded or supported cybersecurity threat information sharing programs,[147] while Ohio FEA suggests that the National Cyber Security Division cyber-response programs under DHS should be included in the PQ List.[148] Microsoft recommends modifying the proposed language to be solution-neutral and outcome-focused to accommodate other timely bi-directional threat information-sharing programs.[149]

75. Microsoft and EEI support the inclusion of internal network security monitoring on the initial PQ List.[150] EEI further recommends that the Commission broaden the eligibility for incentives to cybersecurity capabilities across protective and detective controls, not only those limited to internal network security monitoring.[151] Similarly, SecurityScorecard suggests that the Commission broaden its focus from internal network security monitoring to continuous monitoring so as to secure both the perimeter and internal network.[152] Microsoft supports eligible expenditures associated with internal network security monitoring as cybersecurity best practices consistent with a Zero Trust security model, including technologies associated with asset discovery, inventory and management, network monitoring, traffic classification, and behavior analytics within the internal environment.[153]

76. While acknowledging the cybersecurity benefits of internal network security monitoring, APPA and California Parties do not support its inclusion on the PQ List.[154] California Parties state that utilities have sufficient financial incentives to allocate funding towards internal network security monitoring through the Commission's existing cost recovery mechanisms, and that mandatory CIP Reliability Standards are better suited than incentives for facilitating widespread adoption of internal network security monitoring.[155] APPA argues that internal network security monitoring is not a category of expenditures that can be presumed to materially improve cybersecurity prior to agreement on best practices.[156] In their reply comments, California Parties echo APPA's concerns and note the lack of consensus between commenters as to what qualifies as internal network security monitoring.[157]

77. NERC notes that the CIP Reliability Standards are technology-neutral and do not prescribe specific technological methods, tools, or approaches to reach compliance.[158] NERC states that utilities and other NERC-registered entities may already be using internal network security monitoring in combination with other tools or processes to comply with Reliability Standards and therefore cautions that it may be difficult to determine whether a particular cybersecurity investment is mandatory for purposes of analyzing the second eligibility criterion.

78. UMLARC argues that defense communities face particular cybersecurity risks. UMLARC explains that certain defense communities are implementing community cyber force pilot programs. UMLARC recommends that the Commission place community cyber forces for information-sharing programs on the PQ List, while noting that these programs are still in pilot phases.[159]

79. NERC recommends that the Commission consider the deployment of sensors as part of an operational technology visibility program, administered by the Electricity Information Sharing and Analysis Center (E–ISAC), for inclusion on the PQ List.[160] Microsoft, MISO Transmission Owners,[161] and EEI support the inclusion of internal network security monitoring on the PQ List but recommend that internal network security monitoring expenditures be consistent with a Zero Trust security model.[162] EEI suggests that technology and processes to implement, manage, and monitor user and endpoint behavioral analysis be added to the PQ List.[163]

80. DOE states that the PQ List should be expanded to include other information sharing programs, as well as permit case-by-case basis evaluation of other investments.[164] When considering whether to expand eligible information-sharing programs on the PQ List, DOE recommends that the Commission consider whether investments for participating in other Department-led cybersecurity programs, such as C2M2, materially improve the security posture of the utility.[165] DOE suggests the specific inclusion of the Cybersecurity for the Operational Technology Environment program on the PQ List.[166] EEI broadly suggests that the Commission expand the PQ List to include other federally funded or supported cybersecurity threat information sharing programs.[167]

81. Anterix recommends that the Commission include expenditures for private LTE wireless broadband communication systems as an item eligible for incentives on the PQ List.[168] MISO Transmission Owners and International Transmission Companies

[145] Maryland and Pennsylvania Commissions Initial Comments at 9; California Parties Initial Comments at 7–8.

[146] EEI Initial Comments at 6; UMLARC Initial Comments at 4; Ohio FEA Initial Comments at 7–8.; Microsoft Initial Comments at 2.

[147] EEI Initial Comments at 6.

[148] Ohio FEA Initial Comments at 7–8.

[149] Microsoft Initial Comments at 2.

[150] *Id.;* EEI Initial Comments at 5.

[151] EEI Initial Comments at 5.

[152] SecurityScorecard Initial Comments at 6.

[153] Microsoft Initial Comments at 2.

[154] APPA Initial Comments at 18; California Parties Initial Comments at 13–14.

[155] California Parties Initial Comments at 13–14.

[156] APPA Initial Comments at 18.

[157] California Parties Reply Comments at 10.

[158] NERC Initial Comments at 4–5.

[159] UMLARC Initial Comments at 4.

[160] NERC Initial Comments at 4.

[161] MISO Transmission Owners consist of: Ameren Services Company, as agent for Union Electric Company d/b/a Ameren Missouri, Ameren Illinois Company d/b/a Ameren Illinois and Ameren Transmission Company of Illinois; American Transmission Company LLC; Big Rivers Electric Corporation; Central Minnesota Municipal Power Agency; City Water, Light & Power (Springfield, IL); Cleco Power LLC; Dairyland Power Cooperative; Duke Energy Business Services, LLC for Duke Energy Indiana, LLC; East Texas Electric Cooperative; Entergy Arkansas, LLC; Entergy Louisiana, LLC; Entergy Mississippi, LLC; Entergy New Orleans, LLC; Entergy Texas, Inc.; Great River Energy; GridLiance Heartland LLC; Hoosier Energy Rural Electric Cooperative, Inc.; Indiana Municipal Power Agency; Indianapolis Power & Light Company; Lafayette Utilities Systems; MidAmerican Energy Company; Minnesota Power (and its subsidiary Superior Water, L&P); Montana-Dakota Utilities Co.; Northern Indiana Public Service Company LLC; Northern States Power Company, a Minnesota corporation, and Northern States Power Company, a Wisconsin corporation, subsidiaries of Xcel Energy, Inc.; Northwestern Wisconsin Electric Company; Otter Tail Power Company; Prairie Power, Inc.; Republic Transmission, LLC; Southern Illinois Power Cooperative; Southern Indiana Gas & Electric Company (d/b/a CenterPoint Energy Indiana South); Southern Minnesota Municipal Power Agency; Wabash Valley Power Association, Inc.; and Wolverine Power Supply Cooperative, Inc.

[162] Microsoft Initial Comments at 2; MISO Transmission Owners Initial Comments at 6–7; EEI Initial Comments at 5–6.

[163] EEI Initial Comments at 5–6.

[164] DOE Reply Comments at 6–12.

[165] *Id.* at 10.

[166] *Id.*

[167] EEI Initial Comments at 6.

[168] Anterix Initial Comments at 5.

(ITC Companies) [169] recommend that the Commission add expenditures for utility-owned private fiber networks to the PQ List, as well as expenditures made to upgrade or replace legacy operating systems.[170] They further suggest that the Commission should expand the PQ List to include advanced cybersecurity expenditures to address physical security, such as biometric identification, access cards or access control systems.[171]

82. Microsoft and EEI both recommend inclusion of user and endpoint behavioral analysis.[172] Avangrid and the Operational Technology Cybersecurity Coalition (OT Coalition) advocate for the addition of hardware and software risk management tools aimed to help identify cybersecurity threats to suppliers and vendors.[173] MISO Transmission Owners additionally propose that the Commission expand the PQ List to include cybersecurity expenditures such as for DHS's CyberSentry hardware and software.[174]

83. Microsoft recommends expanding the PQ List to include cloud-enabled security solutions, threat intelligence, vulnerability assessment, access control and privileged access management, endpoint detection and response, firewall and network management, and multifactor authentication and biometrics.[175] EEI suggests that the Commission consider adding technology and processes to develop threat hunting capability within IT and OT environments (*e.g.,* incident response retainer fees, penetration tests, or vulnerability assessments; secure coding practices and consulting services to navigate Software Bill of Materials requirements; and data loss prevention capabilities).[176]

iii. Commission Determination

84. We adopt and modify the NOPR's proposal and add § 35.48(e)(1) to the Commission's regulations to include two cybersecurity investments on the initial PQ List: (1) cybersecurity investments associated with participation in CRISP and (2) cybersecurity investments associated with internal network security monitoring within the utility's cyber systems. We find that both of these cybersecurity investments satisfy the eligibility criteria and both merit the rebuttable presumption.

85. First, we include cybersecurity investments associated with a utility's participation in CRISP. We find that a utility's participation in CRISP materially improves cybersecurity because it involves utility participation in a cybersecurity threat information sharing program. We note that such participation falls under the recommendations in the NIST SP 800–53 Security and Privacy Controls for Information Systems and Organizations catalog. In addition, CRISP: (1) is facilitated by the Federal Government; (2) provides two-way communications from and to electric industry and government entities; and (3) delivers relevant and actionable cybersecurity information to participants within the United States electricity industry. Having found that participation in CRISP satisfies the first eligibility criterion, we include it on the initial PQ List.

86. We are aware that many, but not all, utilities already participate in CRISP. Our inclusion of CRISP on the initial PQ List reflects the mandate in FPA section 291A(c) to establish incentive-based rate treatments by encouraging *participation* in cybersecurity threat information sharing programs. The mandate to incentivize *participation* indicates that all CRISP participants, not just new entrants, should be eligible to seek an incentive for any new cybersecurity investment associated with their participation, so long as that participation is voluntary.

87. Second, we include cybersecurity investments associated with a utility's investment in internal network security monitoring within the utility's cyber systems. As the Commission explained in the NOPR, a utility's cybersecurity investments associated with internal network security monitoring could include IT cyber systems and/or OT cyber systems and could be associated with cyber systems that may or may not be subject to the Reliability Standards.

88. We find that cybersecurity investments associated with internal network security monitoring within the utility's cyber systems materially improves cybersecurity because they are investments in Advanced Cybersecurity Technology. Internal network security monitoring falls under the recommendations in the NIST SP 800–53 Security and Privacy Controls for Information Systems and Organizations catalog. Having found that cybersecurity investments associated with internal network security monitoring within the utility's cyber systems satisfies the first eligibility criterion, we will include it on the initial PQ List.

89. NERC observes that some utilities may already use internal network security monitoring as part of their compliance with Reliability Standards and therefore cautions that it may be difficult to determine whether a particular cybersecurity investment is mandatory for purposes of determining whether such expenditures would qualify for incentive-based rate treatment. We have addressed this concern primarily in section III.A.3.c., and we reiterate that a utility's cybersecurity investments, including internal network security monitoring, made to comply with a Reliability Standard, will not be incentive-eligible because the utility did not make those investments voluntarily. However, there may be instances where a utility invests in internal network security monitoring that while complying with a Reliability Standard also provides enhanced cybersecurity protections that go beyond compliance with a Requirement in the Reliability Standard.[177] Those incremental cybersecurity investments in internal network security monitoring that go beyond compliance with a Requirement in a Reliability Standard would be eligible for incentive-based rate treatment provided that the utility demonstrates that the incremental cybersecurity investments satisfy the eligibility criteria.[178] With regard to NERC's concern regarding the potential difficulty of discerning which cybersecurity investments for internal network security monitoring qualify for incentive-based rate treatment, it is incumbent upon the utility to demonstrate in its filing seeking an incentive that the associated expenses are for new internal network security monitoring that is in addition to its preexisting cybersecurity programs and go beyond compliance with a Requirement in the Reliability Standard.

90. We decline at this time to add any additional cybersecurity investments to

[169] ITC Companies d/b/a ITC*Transmission,* Michigan Electric Transmission Company, LLC, ITC Midwest LLC, and Great Plains, LLC.

[170] MISO Transmission Owners Initial Comments at 6–7; ITC Companies Initial Comments at 5–6.

[171] MISO Transmission Owners Initial Comments at 6–7; ITC Companies Initial Comments at 5–6.

[172] Microsoft Initial Comments at 2; EEI Initial Comments at 6–7.

[173] Avangrid Initial Comments at 6; OT Coalition Initial Comments at 3.

[174] MISO Transmission Owners Initial Comments at 6.

[175] Microsoft Initial Comments at 2.

[176] EEI Initial Comments at 5–6.

[177] *See infra* section III.C.2.c. (discussing the availability of incentive-based rate treatment for *new* cybersecurity investments).

[178] We discuss in section III.D.3.c. the types of information that a utility would need to include in is filing of a request for incentive-based rate treatment for its cybersecurity investment. A utility seeking an incentive-based rate treatment for the incremental voluntary portion of its cybersecurity investment would need to identify its additional, voluntary cybersecurity investments that exceed the legal requirement. The utility would also need to distinguish the portion of the cybersecurity investment it made to comply with a legal requirement from the voluntary portion.

the initial PQ List. Because of the rebuttable presumption afforded to items on the PQ List, it is important that the Commission have a high degree of confidence that such items will likely materially improve cybersecurity for all utilities. While many of the additional cybersecurity investments commenters suggest to include on the initial PQ List may indeed be beneficial investments that would improve cybersecurity, we find that suggestions offered by commenters either lack sufficient evidence to show they will materially improve cybersecurity across all utilities or lack sufficient specificity to be included on the PQ List at this time.

91. As discussed in section III.B.1.a., the Commission will, from time to time, evaluate whether it would be appropriate to modify the PQ List. As the Commission updates the PQ List over time, entities may propose to add the items that the Commission does not accept in this final rule as well as other items, assuming that the entities can provide adequate support as to why it is appropriate to include these items. We also note that we are adding a case-by-case approach in addition to the PQ List approach, and utilities can seek an incentive for these investments on an individual basis, albeit without the presumption of eligibility.

92. In response to SecurityScorecard's suggestion that the Commission broaden its focus from internal network security monitoring to continuous monitoring, we do not agree that the PQ List should be so expanded at this time, as we note that the CIP Reliability Standards already mandate perimeter monitoring in some form. In response to Microsoft and EEI's suggestions, we recognize the benefits of both the Zero Trust security model and deploying Security Information and Event Management processes. However, both are considered to be frameworks that guide cybersecurity investments rather than specific cybersecurity investments themselves. We note that the Commission could consider providing incentives to specific applications of either the Zero Trust security model or Security Information and Event Management on a case-by-case basis, and, in the future, the Commission could consider adding specific applications of these concepts to the PQ List.

93. We disagree with UMLARC that community cyber force informational-sharing programs should be on the PQ List. Community cyber forces are currently pilot programs. By their nature as pilot programs, community cyber forces do not have standardized specific attributes, nor do they have a proven track record for placement on a pre-qualified list. Given that we do not have a clear understanding of these pilot programs or any associated investments, at this time, we decline to add community cyber forces to the PQ List.

94. We disagree with Anterix, MISO Transmission Owners, and ITC Companies' proposals to include investments in private communication systems such as LTE wireless and fiber networks on the PQ List. The use of private communication systems does not necessarily provide a cybersecurity benefit because the confidentiality of data transiting those networks may not be encrypted.

95. The MISO Transmission Owners recommend that the Commission consider adding expenditures associated with the Department of Homeland Security's CyberSentry hardware and software to the PQ List.[179] CyberSentry is a pilot program, and the record in this proceeding does not include enough evidence for us to determine whether CyberSenrty would materially improve the cybersecurity of all utilities. Nevertheless, CyberSentry uses sensors to monitor the IT and OT Networks for cyber security threats, and incentive-based rate treatment for these cybersecurity investments may already be eligible cybersecurity investments as internal network security monitoring.

96. DOE recommends that the Commission consider including the Cybersecurity for the Operational Technology Environment (CyOTE™) program on the PQ List. According to DOE, this program enhances OT threat information-gathering for the energy sector.[180] CyOTE is currently under development, and the record in this proceeding does not include enough evidence for us to determine whether cybersecurity investments associated with CyOTE would materially improve cybersecurity for all utilities. We find that MISO Transmission Owners' and ITC Companies' proposals to include investments made for physical access control systems, access cards, and biometrics are beyond the scope for this proceeding because they are not investments in Advanced Cybersecurity Technology or related to participation in a cybersecurity threat information sharing program. MISO Transmission Owners and ITC Companies also propose including investments for upgrading or replacing legacy systems. We find there is insufficient evidence in the record to determine whether the specific applications could be considered cybersecurity investments. Accordingly, we decline to include these investments on the PQ List.

97. Cybersecurity investments in Advanced Cybersecurity Technology included on the PQ List must include at least one specific security control that materially improves the cybersecurity of all utilities, thus meriting a rebuttable presumption. We find that the proposals from Microsoft and EEI to expand the PQ List to cover a broader set of advanced cybersecurity solutions such as threat intelligence, vulnerability management, access control, and others are vague and lack the specificity needed to establish a record for inclusion on the PQ List. Proposals from Avangrid and the OT Coalition to include investments for hardware and software risk management tools similarly lack specificity. We therefore decline to include these investments on the PQ List at this time.

98. While proposals from EEI to consider investments related to threat hunting, penetration tests, and consulting services for Software Bill of Materials requirements describe efforts to detect cybersecurity vulnerabilities, they also lack specificity with regard to mitigation and remediation of identified deficiencies. Microsoft and EEI both propose including investments for user and endpoint behavioral analysis, and NERC proposes including investments for the deployment of OT sensors. However, commenters do not demonstrate that these items are different in scope than what is already covered by internal network security monitoring on the PQ List. Therefore, we decline to include these investments on the PQ List at this time.

99. As discussed in section III.B.1.a., the Commission will, from time to time, evaluate whether it would be appropriate to modify the PQ List. We also note that, because we are adding a case-by-case approach in addition to the PQ List approach, utilities can seek an incentive for investments not identified

[179] Department of Homeland Security, *ICS Security Offerings Fact Sheet, https://www.cisa.gov/sites/default/files/publications/ics_security_offerings_fact_sheet_S508C.pdf* (explaining that ''CyberSentry is a voluntary pilot program that leverages best in breed, commercial off-the-shelf technologies, such as network intrusion detection tools, to identify malicious activity in Critical infrastructure (CI) ICS and corporate networks. CyberSentry participation increases real-time visibility into U.S. CI and provides the capability to detect nation-state adversaries on CI networks and derive cross-sector analytic insights.'').

[180] DOE, *Cybersecurity for the Operational Technology Environment (CyOTE), https://www.energy.gov/ceser/cybersecurity-operational-technology-environment-cyote* (stating that CyOTE is a ''research initiative, led by CESER in partnership with Idaho National Laboratory and energy sector partners, aims to develop tools and capabilities that can provide energy asset owners and operators with timely alerts and actionable information.'').

on the PQ List, albeit without the presumption of eligibility.

2. Case-by-Case Approach

a. NOPR Proposal

100. In the NOPR, the Commission recognized the limitations of only adopting the PQ List approach and sought comment on whether and, if so, how it should implement a case-by-case approach to grant incentives.[181] The Commission explained that it could permit a utility to file for incentive-based rate treatment for any cybersecurity investment that the utility believes satisfies the eligibility criteria, and that the Commission would review such filings on a case-by-case basis, to determine whether the proposed cybersecurity expenditure satisfies the eligibility criteria.

101. The Commission further explained that its evaluation of a utility's application under the case-by-case approach would differ from its evaluation of a filing seeking incentives for items on the PQ List, although the eligibility criteria would be the same under either approach. Specifically, the case-by-case application would not receive a presumption of eligibility for any cybersecurity investment and the utility would bear the full burden to demonstrate in its filing that its cybersecurity investment meets the eligibility criteria. Just as it would in a filing for incentive treatment of a cybersecurity investment on the PQ List, the filing utility would also need to demonstrate that its proposed rate, inclusive of the incentive, is just and reasonable.

b. Comments

102. OT Coalition, Avangrid, MISO Transmission Owners, EPSA, INGAA, EEI, Microsoft, Ohio Consumers' Counsel, Anterix, and DOE support the adoption of a case-by-case approach in addition to the PQ List approach.[182] Alliant and the Maryland and Pennsylvania Commissions support the adoption of a case-by-case approach instead of the PQ List approach.[183] TAPS, the Michigan Commission, APPA, and California Parties oppose the Commission adoption of a case-by-case approach.[184]

103. EEI, MISO Transmission Owners, INGAA, and Anterix describe the role of a case-by-case approach as a supplement to the PQ List approach, providing flexibility for the filing utilities.[185] Microsoft, OT Coalition, and Ohio Consumers' Counsel highlight the use of the case-by-case approach as a mechanism both for utilities to file for incentives not on the PQ List and to inform additions to the PQ List.[186] INGAA asserts that the case-by-case approach will encourage utilities to make qualifying investments not included on the PQ List, which will result in strengthening the security posture of the Bulk-Power System.[187] Avangrid states that the Commission should allocate sufficient human and financial resources to ensure timely review of case-by-case incentive requests.[188]

104. Alliant and the Maryland and Pennsylvania Commissions support the adoption of a case-by-case approach over the PQ List. Alliant argues that, due to the dynamic and rapid pace at which cybersecurity solutions become obsolete, the case-by-case approach will allow the Commission to review incentive requests in light of the most current technologies available and the overall needs of the utility.[189] The Maryland and Pennsylvania Commissions assert that the case-by-case approach would encourage utilities to be more innovative in their cybersecurity improvements and allows an applicant to demonstrate how a particular incentive addresses the utility's actual needs or meets the statutory criteria specific to the individual utility.[190] Ohio FEA argues that the PQ List approach alone is an inadequate approach because it will be unable to stay abreast of the ever-changing cybersecurity landscape.[191]

105. TAPS, the Michigan Commission, APPA, and California Parties oppose the adoption of the case-by-case approach. The Michigan Commission supports the transparency and efficiency that the PQ List provides over the case-by-case approach.[192] The Michigan Commission argues that, if a cybersecurity investment materially improves security, the investment should be considered for inclusion in the CIP Reliability Standards.[193] TAPS also enumerates concerns with the efficiency and transparency of the case-by-case approach, as well as the potential for increased litigation expenses and slower adoption of Advanced Cybersecurity Technologies.[194] APPA states that the case-by-case approach would be administratively burdensome and lead to incentives for routine, best practice cybersecurity expenditures.[195] California Parties argue that a case-by-case approach would be administratively infeasible and reduce regulatory certainty for filing utilities.[196]

106. The Iowa Utilities Board states that incentives under the case-by-case approach should be higher than those granted under the PQ List because the case-by-case approach drives innovation.[197]

c. Commission Determination

107. We adopt a case-by-case approach to granting incentives by adding § 35.48(e)(2) to the Commission's regulations, which permits a utility to demonstrate that a cybersecurity investment satisfies each of the eligibility criteria. Unlike the PQ List approach, the Commission will not presume that the requested cybersecurity investment satisfies the eligibility criteria. The utility requesting incentive-based rate treatment would need to demonstrate in its filing that the cybersecurity investment(s) would materially improve cybersecurity for the utility requesting the incentive-based rate treatment.

108. We find that allowing utilities to make case-by-case cybersecurity incentive requests in addition to PQ List requests provides several benefits. The case-by-case approach offers greater flexibility than the PQ List approach alone for utilities to respond to cybersecurity threats. In addition, reviewing cybersecurity investments on a case-by-case basis can help to inform the Commission about potential new additions that it could make to the PQ List in future proceedings. We believe

[181] NOPR, 180 FERC ¶ 61,189 at P 32.

[182] OT Coalition Initial Comments at 2–3; Avangrid Initial Comments at 5, 6. MISO Transmission Owners Initial Comments at 4; EPSA Initial Comments at 5; INGAA Initial Comments at 4; EEI Initial Comments at 4–5; Microsoft Initial Comments at 2; Ohio Consumers' Counsel Initial Comments at 9; Anterix Initial Comments at 12–13; Anterix Reply Comments at 12; DOE Reply Comments at 10.

[183] Alliant Initial Comments at 4–5; Maryland and Pennsylvania Commissions Initial Comments at 7–8.

[184] TAPS Initial Comments at 7; Michigan Commission Initial Comments at 6; APPA Initial Comments at 5; California Parties Initial Comments at 31–32; California Parties Reply Comments at 12–13.

[185] EEI Initial Comments at 4–5; MISO Transmission Owners Initial Comments at 4; INGAA Initial Comments at 4; Anterix Initial Comments at 12–13; Anterix Reply Comments at 12.

[186] Microsoft Initial Comments at 2; OT Coalition Initial Comments at 2, 3; Ohio Consumers' Counsel Initial Comments at 9.

[187] INGAA Initial Comments at 4.

[188] Avangrid Initial Comments at 4.

[189] Alliant Initial Comments at 4–5.

[190] Maryland and Pennsylvania Commissions Initial Comments at 7–8.

[191] Ohio FEA Initial Comments at 9.

[192] Michigan Commission Initial Comments at 6.

[193] *Id.* at 9.

[194] TAPS Initial Comments at 7–9.

[195] APPA Initial Comments at 17.

[196] California Parties Initial Comments at 31–32.

[197] Iowa Utilities Board Initial Comments at 5–6.

that, by allowing utilities to use more than one approach to show that a cybersecurity investment satisfies the eligibility criteria, we strike the right balance between customer protection, transparency, efficiency, and responsiveness to cybersecurity threats.

109. In order to determine on a consistent and transparent basis whether a cybersecurity investment satisfies the first eligibility criterion, the Commission will consider evidence showing that the utility would invest in cybersecurity improvements that: (1) are based on a documented and recommended technical cybersecurity mitigation action published in an alert or advisory by a relevant Federal agency (*e.g.,* CISA, DOE, FBI, DOD, NSA); [198] and (2) respond to an alert or advisory that meets the objective of a subcategory of the NIST Cybersecurity Framework, or its successor, and references the related NIST 800–53 Security Control, or its successor.[199] The Commission would base its assessment of the evidence on whether an incentive is appropriate on the mitigation actions detailed in the specified agencies' alerts and advisories along with the NIST Cybersecurity Framework and NIST 800–53 Security Controls to determine whether the utility's proposed cybersecurity investment would materially improve its cybersecurity.

110. As discussed in section III.A.3. and consistent with the Commission's evaluations of PQ List cybersecurity investments in section III.B.1.a., under the case-by-case approach a utility would still need to demonstrate that it would make the cybersecurity investment voluntarily, and that the proposed rate, including the cybersecurity incentive, is just and reasonable and not unduly discriminatory or preferential.

111. We decline to add any additional eligibility criteria to our regulations that would apply only to cybersecurity investments that are not included on the PQ List. We find that the eligibility criteria in our regulations are sufficient for incentive requests that use either the PQ List or case-by-case approach. Similarly, we decline to offer different forms of incentives for cybersecurity investments based on whether or not the investment appears on the PQ List. We are not convinced that the benefits of cybersecurity investments made that are on the PQ List or for which a utility requests incentives on a case-by-case basis differ and would therefore merit disparate incentive levels because all incentive-eligible investments under both mechanisms must satisfy the requirement to materially improve cybersecurity in the first eligibility criterion.

3. Early Compliance With Approved Reliability Standards

a. NOPR Proposal

112. In the NOPR, the Commission proposed the second eligibility criterion limiting incentive-based rate treatment to cybersecurity investments that a utility made voluntarily.[200] The NOPR also sought comment on whether the second eligibility criterion was appropriate and whether there were additional criteria or limitations that the Commission should consider, including any potential refinements, and any other criteria for incentive eligibility that the Commission should adopt in the final rule. Finally, the NOPR proposed to allow a utility granted a cybersecurity incentive to receive that incentive until the investment or activity that serves as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission.[201] This would include cybersecurity investments made by a utility to comply with Reliability Standards that the Commission has already approved pursuant to § 39.5(d) of the Commission's regulations, but that have not yet taken effect pursuant to the implementation plan approved by the Commission.

b. Comments

113. Many commenters discuss how the NOPR's proposed incentives would interact with and affect the CIP Reliability Standards and development processes. Indicated PJM Transmission Owners, the Michigan Commission, and EPSA note that incentives could supplement the time-intensive NERC standards development process.[202] APPA and Alliant express concern that providing incentives for cybersecurity investments would disincentivize the timely development of CIP Reliability Standards.[203] NERC advises the Commission to develop rate incentives for voluntary cybersecurity investments that build upon and complement existing CIP Reliability Standards.[204] NERC and TAPS advise the Commission to consider how the proposed incentives will affect compliance with the CIP Reliability Standards.[205]

114. Indicated PJM Transmission Owners support the availability of incentives to early adopters of cybersecurity technology.[206] The Michigan Commission discusses an approach in which the proposed Cybersecurity Regulatory Asset Incentive would be used to facilitate cybersecurity investments during the period in which said investments are evaluated for inclusion in the CIP Reliability Standards.[207] EPSA notes that the nature of the long, detailed process to develop and implement NERC CIP Reliability Standards may not be able to keep up with the rapidly evolving nature of cybersecurity threats.[208] EPSA states that it is prudent to provide incentives for protections to address rapidly evolving technologies to ensure a reliable, resilient, and operational electric grid.[209]

115. The Maryland and Pennsylvania Commissions argue that making incentives available in the period before the completion of mandatory standards does not expedite the standards process or the voluntary adoption of improvements.[210] On the contrary, they assert that the proposed incentives actually would encourage delays in the standards development process so utilities could recover incentives for voluntary implementation.[211] The Maryland and Pennsylvania Commissions further note that the proposed incentives do not provide a tapering off period, such as over the time frame in which a CIP Reliability Standard is being developed. They assert that such a tapering period would

[198] Technical cybersecurity mitigation action means a recommended action requiring the purchase of software, hardware, or third-party services.

[199] Some alerts may reference specific NIST 800–53 Security Controls, while others may reference security controls generally. One example of a case-by-case request for incentive-based rate treatment of cybersecurity investments is a utility requesting an incentive for an implementation of data backup procedures on both the IT and OT networks. This type of action is specifically recommended in the CISA ''Shields Up'' Alert. *See* CISA, *Essential Element: Your Data* (Oct. 15, 2020), *https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%205%2020201015_508.pdf.* Further, this action is covered by the NIST Cybersecurity Framework Category Information Protection Processes and Procedures, subcategory 4 and thus would be evidence that this proposed implementation would materially improve the utility's cybersecurity.

[200] *Id.* PP 20, 22.

[201] *Id.* P 46.

[202] Indicated PJM Transmission Owners Initial Comments at 5; Michigan Commission Initial Comments at 9; EPSA Initial Comments at 2.

[203] APPA Initial Comments at 13–14; Alliant Initial Comments at 7–8.

[204] NERC Initial Comments at 3.

[205] *Id.* at 4; TAPS Initial Comments at 12.

[206] Indicated PJM Transmission Owners Initial Comments at 5.

[207] Michigan Commission Initial Comments at 9.

[208] EPSA Initial Comments at 2.

[209] *Id.*

[210] Maryland and Pennsylvania Commissions Initial Comments at 10.

[211] *Id.* at 10.

motivate utilities to implement material improvements as early as possible.[212]

116. APPA recommends that the Commission modify the proposed eligibility criteria in a manner that would disallow incentives for early adoption of CIP Reliability Standards.[213] Instead of a cybersecurity expenditure losing eligibility when it becomes mandatory pursuant to a CIP Reliability Standard, APPA recommends that the cut off for incentives should be the earlier of: (1) the date of any Commission directive that would require the investment; or (2) the date that a Standards Authorization Request is submitted to NERC to require that incentive.[214] APPA argues that it would not be just or reasonable to provide an incentive to a utility for an investment where a new or revised mandatory Reliability Standard is pending.[215]

c. Commission Determination

117. We adopt an application of the case-by-case method for utilities to satisfy the eligibility criteria by adding § 35.48(e)(3) to the Commission's regulations, which permits utilities to receive incentives for cybersecurity investments made to comply with a cybersecurity-related CIP Reliability Standard (*i.e.,* excluding CIP Reliability Standards that may be related to physical security and not cybersecurity) approved by the Commission before that CIP Reliability Standard becomes mandatory and enforceable for that utility. In general, cybersecurity investments made by a utility to comply and maintain its compliance with a Commission-approved Reliability Standard will materially improve the utility's cybersecurity. Filing utilities would need to demonstrate that the cybersecurity investment(s) it will make are necessary to comply with the Reliability Standard, and that it will make those cybersecurity investments prior to the date that the Reliability Standard is mandatory and enforceable for that utility.[216] Those cybersecurity investments made by the utility before the newly-approved Reliability Standard becomes effective (*i.e.,* mandatory and enforceable) are voluntary. Those cybersecurity investments made by the utility after the newly-approved Reliability Standard becomes effective and mandatory are no longer voluntary. As required by the second eligibility criteria, all of the utility's cybersecurity investments incurred to comply with a Reliability Standard after the Reliability Standard becomes mandatory and enforceable for that utility are ineligible for incentive-based rate treatment.

118. We find that allowing utilities to receive an incentive to comply with a Commission-approved cybersecurity-related CIP Reliability Standard before it becomes mandatory and enforceable could materially improve their cybersecurity posture during that period. In addition, we find that permitting an incentive for early compliance with approved cybersecurity-related CIP Reliability Standards will help to bridge gaps between voluntary cybersecurity measures and the cybersecurity measures mandated in the CIP Reliability Standards. It is possible that allowing utilities to receive incentives for early compliance could unintentionally incentivize standards drafting teams' artificial lengthening of the implementation period to increase the amount of time a utility could receive incentives. Nevertheless, the Commission would continue to consider whether the implementation time is reasonable when determining whether to approve the proposed CIP Reliability Standard.[217]

119. We clarify that the cybersecurity investments made by a utility to achieve early compliance with an approved cybersecurity-related CIP Reliability Standard may be eligible for incentive-based rate treatment. We reiterate that, after receiving Commission authorization for incentive-based rate treatment, the utility may only collect the incentive during the period that begins with the utility achieving compliance with the approved cybersecurity-related CIP Reliability Standard and that ends according to the duration provisions of § 35.48(g), as further discussed in section III.D.[218] Therefore, the earlier that a utility complies with a new CIP Reliability Standard, the longer the utility's incentive recovery period may be.

C. Cybersecurity Investment Rate Incentives

120. The Commission proposed two potential rate incentive options for utilities that make eligible cybersecurity investments: (1) the Cybersecurity ROE Incentive, an ROE adder of 200 basis points that would be applied to the incentive-eligible investments; [219] and (2) the Cybersecurity Regulatory Asset Incentive, 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.[220] The Commission stated that both offer meaningful incentives to encourage cybersecurity investments that improve a utility's cybersecurity posture.[221] The Commission also sought comment on whether, and if so how, the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.[222]

121. The Commission also noted that most utility IT investments (general and intangible plant) and expenses (administrative and general costs) support functions of the entire utility, not just the transmission function.[223] Consequently, the Commission found that only a portion of those costs are allocated to transmission customers, typically based on wages and salaries allocators.[224]

1. Cybersecurity ROE Incentive

a. NOPR Proposal

122. The Commission proposed to allow a utility that makes cybersecurity investments that are eligible for incentives to request the Cybersecurity ROE Incentive that would be applied to the incentive-eligible investments.[225] The Commission explained that any

[212] *Id.* at 10.

[213] APPA Initial Comments at 13–14.

[214] *Id.* at 13–14.

[215] *Id.* at 13–14.

[216] In addition, as explained below, filings seeking the incentives would have to comply with the filed rate doctrine. *See Exxon Mobil Corp.* v. *FERC,* 571 F.3d 1208, 1211 (D.C. Cir. 2009) (citing *Towns of Concord, Norwood, & Wellesley* v. *FERC,* 955 F.2d 67, 71 & n.2 (D.C. Cir. 1992); *Ark. La. Gas Co.* v. *Hall,* 453 U.S. 571, 577–578 (1981)) (''The Commission may not retroactively alter a filed rate to compensate for prior over- or underpayments. A corollary to this rule against retroactive ratemaking, the filed rate doctrine, forbids a regulated entity to charge rates for its services other than those properly filed with the appropriate regulatory authority. Together, these rules generally limit the relief the Commission may order to prospective [rates].'') (cleaned up).

[217] *See Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, & Enf't of Elec. Reliability Standards,* Order No. 672, 71 FR 8662 (Feb. 17, 2006), 114 FERC ¶ 61,104, at P 333, *order on reh'g,* Order No. 672–A, 71 FR 19814 (Apr. 18, 2006), 114 FERC ¶ 61,328 (2006) (''In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply'').

[218] In addition to having its rate that includes incentive-based treatment on file with the Commission, a utility must submit an informational filing to the Commission notifying the Commission of the date that it has achieved compliance with the approved cybersecurity-related CIP Reliability Standard.

[219] NOPR, 180 FERC ¶ 61,189 at P 36.

[220] *Id.* P 39.

[221] *Id.* P 33.

[222] *Id.* P 45.

[223] *Id.* P 36.

[224] *Id.* P 36.

[225] *Id.* P 36.

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.[226] The Commission stated that the 200-basis point ROE adder would provide a meaningful incentive to encourage utilities to improve their systems' cybersecurity. The Commission recognized that this amount exceeds the ROE incentives for transmission facilities that the Commission typically provides pursuant to FPA section 219. The Commission explained that, because cybersecurity investments are relatively small compared to conventional transmission projects, a higher ROE may be necessary to affect the expenditure decisions of utilities, without unduly burdening ratepayers.

123. The Commission also proposed that enterprise-wide investments, which are not specific to transmission or the sale for resale of electric energy in interstate commerce, but a portion of which are recovered through rates on file with the Commission, 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.[227] However, consistent with both longstanding cost-causation ratemaking principles [228] and the statutory requirement that rates inclusive of incentives be just and reasonable and not unduly discriminatory or preferential, the Commission proposed 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.

b. Comments

124. EEI, MISO Transmission Owners, and Indicated PJM Transmission Owners support the proposed ROE incentive.[229] EEI notes that some cybersecurity investments involve relatively low dollar amounts, compared with other capital investments.[230] Therefore, in addition to the fact that these investments are recovered over a short period, EEI believes that the proposed 200-basis point adder is reasonable and has the potential to create an incentive that will shift utility cybersecurity expenditures in the manner intended by the Commission and Congress.[231]

125. EEI and MISO Transmission Owners support the Commission's proposal to include enterprise-wide costs as eligible for incentive treatment.[232] EEI states that 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.[233] MISO Transmission Owners state that the inclusion of enterprise-wide costs encourages enterprise-wide strategic security investments, which provide benefits to a utility's security program efficiency more broadly, as well as to ratepayers.[234]

126. APPA and Alliant agree with the proposal in the NOPR to cap total base and incentive ROE at the top of the zone of reasonableness.[235] APPA asks the Commission to clarify that, in applying the cap at the top end of the zone of reasonableness, a public utility would be required to take into account ROE adders other than the cybersecurity investment adder.[236]

127. Alliant, APPA, Iowa Utilities Board, Joint Consumer Advocates, the Michigan Commission, Ohio FEA, Ohio Consumers' Counsel, and TAPS do not support the proposed ROE adder of 200 basis points.[237] Alliant, APPA, California Parties, Ohio Consumers' Counsel, and Ohio FEA argue that the proposed 200-basis points adder is not just and reasonable.[238] APPA, California Parties, and TAPS also argue that the Commission has not sufficiently supported or explained why a 200-basis point return is necessary.[239]

128. APPA, California Parties, and TAPS argue that eligible cybersecurity investments are not ''relatively small'' as the NOPR suggests.[240] California Parties state that, in recent years, the California Public Utilities Commission has authorized significant amounts for State jurisdictional cybersecurity capital expenditures and annual IT physical and cybersecurity activities for utilities.[241] TAPS comments that the Commission has found that Duke Energy has made over $137 million in capital investments as part of its cybersecurity program that is designed based on the NIST Framework.[242] TAPS further states that, in 2019, Dominion Energy Virginia received State approval to spend $910.3 million on cyber and physical security and telecommunications over 10 years, with $154.4 being spent in the first three years related to improved monitoring and alarm capabilities and enhanced utility security.[243] TAPS argues that these sums illustrate that cybersecurity investments are not relatively small compared to conventional transmission projects.[244]

129. The Michigan Commission states that the potential financial risks that cyberattacks can pose on electric utilities already serve as a strong incentive for investment, much stronger than an additional 200 basis points would provide when applied to what the NOPR recognizes are relatively low-cost investments.[245]

130. Alliant states that using a 200-basis point ROE incentive would impose unnecessary administrative burdens on the Commission and all parties affected, as processing requests for incentives would consume valuable and limited resources of the Commission.[246] Iowa Utilities Board argues that an incentive rate adder could have a cascading impact on

[226] *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).

[227] NOPR, 180 FERC ¶ 61,189 at P 37.

[228] *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).

[229] EEI Initial Comments at 9; MISO Transmission Owners Initial Comments at 10; Indicated PJM Transmission Owners Initial Comments at 4.

[230] EEI Initial Comments at 9–10.

[231] *Id.* at 9–10.

[232] MISO Transmission Owners Initial Comments at 10.

[233] EEI Initial Comments at 10.

[234] MISO Transmission Owners Initial Comments at 10–11.

[235] APPA Initial Comments at 19; Alliant Initial Comments at 6.

[236] APPA Initial Comments at 19.

[237] Alliant Initial Comments at 6, APPA Initial Comments at 10; Iowa Utilities Board Initial Comments at 4; Joint Consumer Advocates Initial Comments at 3; Michigan Commission at 9; Ohio FEA Initial Comments at 10; TAPS Initial Comments at 16.

[238] Alliant Comments at 5–6; California Parties Initial Comments at 22; ITC Companies Initial Comments at 3; Joint Consumer Advocates Initial Comments at 3; Michigan Commission Initial Comments at 9; Ohio Consumers' Counsel Initial Comments at 12; Ohio FEA Initial Comments at 11.

[239] Alliant Comments at 5–6; APPA Initial Comments at 11; California Parties Initial Comments at 22; Ohio Consumers' Counsel Initial Comments at 12; Ohio FEA Initial Comments at 11.

[240] APPA Initial Comments at 11; California Parties Initial Comments at 23; TAPS Initial Comments at 17.

[241] California Parties Initial Comments at 23.

[242] TAPS Initial Comments at 17.

[243] *Id.* at 17.

[244] *Id.* at 17.

[245] Michigan Commission Initial Comments at 8–9.

[246] Alliant Initial Comments at 6.

economic activity, might adversely impact inflation, and could provide a perverse incentive to invest in unneeded technologies.[247] Ohio Consumers' Counsel comments that a 200-basis point adder is not necessary and is unreasonably costly for consumers, and also defies the logic of Order No. 679, which contemplated ROE adders of 100 and 150 basis points only, with the higher ROEs for more complicated and expensive transmission projects.[248]

131. Several commenters argue for a modification to the Commission's proposal of 200 basis points. NRECA requests that the Commission revise its proposal to allow for a request of up to 200-basis points, and questions whether it is appropriate to grant the same ROE adder for all cybersecurity expenditures or whether the Commission instead should tie the amount of the ROE incentive to the projected impact of the cybersecurity expenditure.[249] APPA asks whether the Commission has considered whether applying a smaller ROE adder would be sufficient to encourage investment.[250] Ohio Consumers' Counsel states that, instead of proposing a flat 200-basis point ROE adder, the Commission should provide for a pool of potential adders, ranging from 25 basis points up to a cap of 50 basis points, depending on the magnitude of the investment and the complexity or proven track record for the technology or activity.[251]

132. The Maryland and Pennsylvania Commissions suggest tapering incentives over time to encourage utilities to implement material improvements as early as possible. They argue that such tapering adds a ''performance-based'' aspect to the NOPR proposals.

133. AEP and ITC Companies request that the Commission apply incentives to the entire rate base.[252] ITC Companies state that it might be better to offer a general rather than asset-specific ROE adder for utilities that adopt a sufficient level of additional Advanced Cybersecurity Technologies and cybersecurity threat information sharing program participation.[253] ITC Companies argue that this would reflect the fact that an entity's individual cybersecurity assets and practices are part of a cohesive defensive framework that applies to its entire operation.[254] ITC Companies explain that the type of cybersecurity investment to which the ROE incentive might apply is not a financially significant portion of total rate base for most responsible entities and, in many instances, it is likely that the marginal benefit of this incentive will not justify the administrative cost of obtaining this incentive (even with a PQ List in place), especially where the zone of reasonableness applicable to a responsible entity's overall rate of return further diminishes the impact of the incentive.[255] AEP argues that an incentive adder applied system-wide to the transmission rate base would not need to rise to the level contemplated in the NOPR, *e.g.,* 50 basis points, and would be sufficient to incentivize industry participants to adopt cybersecurity programs that go above and beyond existing cybersecurity requirements.[256]

c. Commission Determination

134. We decline to adopt an ROE incentive adder, as proposed in the NOPR. We conclude that the Cybersecurity Regulatory Asset Incentive satisfies the statutory obligation to benefit consumers by encouraging investments by utilities in Advanced Cybersecurity Technology and participation by utilities in cybersecurity threat information sharing programs. We believe that expenses, which include cybersecurity assessments, architectural reviews, maturity model evaluations, software subscriptions, monitoring, training, procuring outside services, and cloud computing services, constitute a large portion of overall expenditures for many cybersecurity investments, including cybersecurity threat information sharing programs. We find that the provision of the Cybersecurity Regulatory Asset Incentive alone provides the encouragement that Congress intended without unduly increasing costs on consumers.

2. Cybersecurity Regulatory Asset Incentive

a. NOPR Proposal

135. The Commission proposed a Cybersecurity Regulatory Asset Incentive to allow a utility that makes cybersecurity investments that are eligible for incentives to seek deferred cost recovery.[257] The Commission explained 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. 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, the Commission proposed 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. The Commission also sought comment on whether it would be preferable to permit only 50% of incentive-eligible expenses to be treated as regulatory assets.

136. The Commission observed that a range of implementation costs associated with cybersecurity investments could be eligible for deferred rate treatment.[258] Such costs may include, for example, training to implement new cybersecurity practices and systems. However, the Commission proposed 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. The Commission stated that another potentially eligible implementation cost may be internal system evaluations and assessments or analyses by third parties, to the extent that they are associated with a capitalizable item and are part of eligible capitalizable costs. The Commission proposed 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 may include, for example, subscriptions, service agreements, and post-implementation training costs. Specifically, the Commission proposed to allow utilities, under this incentive, to include ongoing dues and other expenses directly associated with participation by utilities in cybersecurity threat information sharing programs that satisfy the eligibility criteria.

[247] Iowa Utilities Board Initial Comments at 4.

[248] Ohio Consumers' Counsel Initial Comments at 12–13.

[249] NRECA Initial Comments at 10.

[250] APPA Initial Comments at 11.

[251] Ohio Consumers' Counsel Initial Comments at 13.

[252] AEP Initial Comments at 6; ITC Companies Initial Comments at 4.

[253] ITC Companies Initial Comments at 4.

[254] *Id.* at 4.

[255] *Id.* at 3.

[256] AEP Initial Comments at 6.

[257] NOPR, 180 FERC ¶ 61,189 at P 39.

[258] *Id.* P 40.

137. The Commission observed that, because FPA section 219A(c)(2) directs the Commission to offer incentives to encourage *participation* by public utilities in cybersecurity threat information sharing programs, it proposed to allow utilities that are currently participating in such programs to seek incentives for any new cybersecurity investment associated with their participation, so long as that participation is voluntary.[259] The Commission sought comment on whether to allow utilities who are already participating in an eligible cybersecurity threat information sharing program to be eligible for this incentive.[260]

138. The Commission also noted that the Commission's rules and regulations in the Uniform System of Accounts [261] 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.[262] The Commission explained that, pursuant to its existing regulations, utilities must maintain sufficient records to support the distinction of any investments that are afforded incentive-based rate treatment.[263]

139. Additionally, the Commission proposed that only directly-assigned utility costs or the conventionally allocated portion of enterprise-wide expenses (*e.g.,* using the wages and salaries allocator) would be eligible for the Cybersecurity Regulatory Asset Incentive in rates on file with the Commission.[264]

b. Comments

140. EEI, Iowa Utilities Board, the Michigan Commission, and MISO Transmission Owners support the Commission's proposal.[265] The Michigan Commission states that the Commission's acknowledgement that many cybersecurity costs have shifted to expenses rather than capital costs is valid.[266] The Michigan Commission adds that the proposed Cybersecurity Regulatory Asset Incentive could help facilitate these types of investments during the time in which such investments are evaluated for inclusion in the CIP Reliability Standards, and that the proposed Cybersecurity Regulatory Asset Incentive would allow for reasonable facilitation of cybersecurity investments in advance of CIP Reliability Standard updates and would avoid unjust and unreasonable rates.[267] Iowa Utilities Board comments that allowing a utility to capitalize the operational expenses for cybersecurity expenditures is by itself an adequate incentive because it reduces cash flow demands and provides an opportunity for the utility to earn a return on those expenditures.[268]

141. MISO Transmission Owners support the proposal to allow utilities to defer and amortize eligible costs that are typically recorded as expenses that are associated with third-party hardware, software, and computing and networking services.[269] MISO Transmission Owners state that allowing transmission owners to capitalize costs and investments associated with cybersecurity investment, including up-front training and implementation expenses, will enable utilities to fully realize the relative security benefits that rapid adoption of cybersecurity investment can generate, as well as the often-lower cost that such solutions impose on ratepayers relative to physical infrastructure.[270]

142. MISO Transmission Owners ask the Commission to clarify that cybersecurity-related operation and maintenance expenses, labor costs, and post-implementation training costs may be included as part of the Cybersecurity Regulatory Asset Incentive.[271] 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.[272] EEI expresses concern 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.[273] EEI argues that 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.[274]

143. Ohio Consumers' Counsel opposes the proposal to allow deferred accounting and recovery of a return on the unamortized portion of the costs for cybersecurity expenses.[275] Ohio Consumers' Counsel states that deferred accounting and cost collection of cybersecurity expenses as regulatory assets will cost consumers more over time than would recovery of the expense all in one year.[276]

144. APPA and California Parties contend that the Cybersecurity Regulatory Asset Incentive should be limited to 50% of eligible investment in cybersecurity initiatives.[277] California Parties comment that the Commission should allow no more than 50% of eligible expenses to be treated as a regulatory asset included in transmission rate base to reduce the burden on consumers.[278] California Parties argue that the Commission failed to offer any explanation as to why its proposal that 100% of eligible expenses should be able to receive incentive treatment is properly calibrated to induce the desired investment.[279]

c. Commission Determination

145. We adopt the NOPR's proposal to add § 35.48(f) to the Commission's regulations to include a Cybersecurity Regulatory Asset Incentive that allows a utility to seek deferred cost recovery for cybersecurity investments that are eligible for incentives. We find that, in limited circumstances that are specific to cybersecurity investments, it is 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 the utility's rate base.

146. In response to Ohio Consumers' Counsel's concerns about consumer costs, as an initial matter, we note that increased consumer costs in isolation do not impugn the reasonableness of an incentive, provided the rates are still just and reasonable. The Commission has long offered transmission incentives, which increase rates, because they encourage investments and activities that the Commission has found provide consumer benefits. The Cybersecurity Regulatory Asset

[259] *Id.* P 41.

[260] *Id.* P 41.

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

[262] NOPR, 180 FERC ¶ 61,189 at P 42.

[263] *Id.*

[264] *Id.* P 43.

[265] EEI Initial Comments at 11; Iowa Utilities Board Initial Comments at 3–4; Michigan Commission Initial Comments at 9; MISO Transmission Owners Initial Comments at 11.

[266] Michigan Commission Initial Comments at 9.

[267] *Id.*

[268] Iowa Utilities Board Initial Comments at 4.

[269] MISO Transmission Owners Initial Comments at 11.

[270] *Id.*

[271] *Id.*

[272] EEI Initial Comments at 11.

[273] *Id.* at 11.

[274] *Id.* at 11–12.

[275] Ohio Consumers' Counsel Initial Comments at 10.

[276] *Id.*

[277] APPA Initial Comments at 12; California Parties Initial Comments at 24.

[278] California Parties Initial Comments at 24.

[279] *Id.* at 24.

Incentive nominally increases rates, though consumers benefit from the time value of money associated with later recovery through rate base than immediate recovery as an expense. Based on the expense-heavy nature of many cybersecurity investments, we find this appropriate to effectuate Congress' requirement that the Commission offer cybersecurity incentives. We also will not, as suggested by California Parties and APPA, limit this incentive to 50% of eligible expenses. Given the comparatively small amount of many cybersecurity expenses, we find that such a limitation may inadequately provide incentives to meaningfully encourage utilities to improve their cybersecurity posture.

147. In response to MISO Transmission Owners' and EEI's comments, we clarify that utilities may seek this incentive for a range of expenses including operation and maintenance expenses, labor costs, implementation costs, network monitoring, and training costs. Additionally, ongoing expenses, either incurred by utility employees or utility payments to third parties may be eligible. Software purchases typically would not qualify for the Cybersecurity Regulatory Asset Incentive because they generally constitute capital investments; however, software-as-a-service expenses could qualify for the Cybersecurity Regulatory Asset Incentive.

148. We find it appropriate to limit eligibility for incentive-based rate treatment to new cybersecurity investments. As also discussed in section III.D.3.c., we add § 35.48(h)(5) to our regulations to provide that the Cybersecurity Regulatory Asset Incentive may be applied to new cybersecurity investments that: (1) occur after the effective date of the Commission's approval of incentive-based rate treatment; and (2) are materially different from cybersecurity investments already incurred by the utilities more than three months prior to the incentive request. Utilities may seek incentives for one-time cybersecurity expenses and/or recurring ones.

149. We generally define new cybersecurity investments to include investments for those activities that have occurred no more than three months prior to the date that the utility files its incentive request with the Commission. We provide one exception and one clarification to this general three-month rule. First, a utility may seek incentive-based rate treatment for its future cybersecurity investments made to participate in cybersecurity threat information sharing programs even if the utility began its participation and therefore made cybersecurity investments related to its participation more than three months before filing its request for incentive-based rate treatment with the Commission. We clarify that utilities seeking incentive-based rate treatment for cybersecurity investments made to comply with a Commission-approved cybersecurity-related CIP Reliability Standard before it becomes mandatory and enforceable for that utility will be permitted to seek incentive-based rate treatment for its cybersecurity expenses that began no earlier than three months before the date that the Commission's approval of the Reliability Standard becomes effective. A utility's cybersecurity expenses that began more than three months before the date that the Commission order or final rule approving a new or modified Reliability Standard becomes effective will not be considered new and will be considered materially similar and duplicative. Therefore, the cybersecurity investments made more than three months before the Commission approves a new or modified Reliability Standard would be ineligible to receive incentive-based rate treatment as early compliance with an approved Reliability Standard.

150. To be clear, this prior three-month provision only determines whether a utility's cybersecurity investment is new and therefore eligible for incentive-based rate treatment. The filed rate doctrine and the rule against retroactive ratemaking preclude the Commission from granting a utility incentive-based rate treatment for cybersecurity investments made before the Commission acts on a request for declaratory order or the effective date of an FPA section 205 filing requesting the incentive-based rate treatment for cybersecurity incentives.[280]

151. Moreover, we find it appropriate that only new cybersecurity investments, and not duplicative or materially similar ones to existing expenses, be eligible. As discussed in section III.D.3., we will require utilities to attest that the cybersecurity investments that are the basis for the incentive-based rate treatments are new cybersecurity investment and not duplicative or materially similar to preexisting expenses. For instance, investment in training associated with a new cybersecurity system may be eligible while annual basic cybersecurity training may not, even if the contents slightly change year-to-year. This will ensure that incentives encourage cybersecurity investments that improve a utility's cybersecurity posture rather than just reward ongoing or recurring activities. The three-month period to determine eligibility of incentives for pre-existing expenses allows for utilities making new cybersecurity investments to respond to immediate cybersecurity vulnerabilities while giving them time to request incentives. We reiterate that utilities may not recover incentives on specific investments that predate the effective date of filing requesting incentive-based rate treatment. We find that this grace period could incentivize utilities not to wait until the effective date of requested incentives to undertake urgent cybersecurity action.

152. FPA section 219A(c)(2) requires the Commission to offer incentives to encourage *participation* by public utilities in cybersecurity threat information sharing programs. Furthermore, participation in information-sharing programs provides cybersecurity benefits to the participating utility that applies for an incentive-based rate treatment, the other program participants, and their customers. Consequently, unlike other expenses, we find that utilities may request the Cybersecurity Regulatory Asset Incentive for expenses associated with participation in cybersecurity threat information sharing programs regardless of how long the utilities have participated in the programs—although only expenses prospective from the effective date of the Commission's approval of the cybersecurity incentives in the utility's rate(s) on file with the Commission shall be eligible.

153. The Commission's rules and regulations in the Uniform System of Accounts[281] 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. Pursuant to our existing regulations, any utility receiving an incentive must maintain sufficient records to support the distinction of any investments that are afforded incentive-based rate treatment.[282] Given the novelty of allowing incentive recipients to include certain expenses in rate base, it is essential that the utilities keep records in a manner that allows the Commission and other parties to ensure that no double-recovery occurs.

[280] *See* n.216, *supra.*

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

[282] *Id.*

154. We also find that, consistent with the Commission's longstanding cost-causation ratemaking principles, only costs directly assigned to a function or the conventionally allocated portion of enterprise-wide expenses (*e.g.,* using the wages and salaries allocator) would be eligible for the Cybersecurity Regulatory Asset Incentive in rates specific to that function. For example, only incentives for transmission-specific or transmission-allocated costs may be recovered in transmission rates.

3. Performance-Based Rates

a. NOPR Proposal

155. In the NOPR, the Commission noted that FPA section 219A(c) directs the Commission to establish incentive-based, including performance-based, rate treatments.[283] The Commission observed that, 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. The Commission explained that performance-based ratemaking can take multiple forms, but ultimately requires the ability to measure and tie rate treatments to actual performance.[284]

156. The Commission sought comment on performance-based rates and whether and how the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.[285] The Commission also sought comment on specific cybersecurity performance metrics that could be subject to a performance standard.[286] In particular, the Commission sought comment on whether any widely accepted metrics for cybersecurity performance could lend themselves as benchmarks for performance-based rates, or whether new appropriate metrics could be developed. The Commission further sought comment on what rate mechanisms could accompany such metrics. The Commission asked 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.

b. Comments

157. No commenter explicitly supports performance-based rates with respect to cybersecurity investments. EEI, Iowa Utilities Board, and Ohio Consumers' Counsel all filed comments opposing this approach.[287] EEI argues that, without clear, industry-wide metrics, a performance-based program would be difficult to implement.[288] Ohio Consumers' Counsel states that setting a performance threshold for advanced cybersecurity investment and activities is likely to be challenging, given the rapid pace of development in both the types of cybersecurity threats experienced and the technological advances used to counter those threats.[289] Iowa Utilities Board comments that performance measurement for cybersecurity investments is difficult because, more often than not, it would be difficult to pinpoint the root cause of failure on a particular entity or process when there is a performance failure.[290]

158. Ohio FEA states that, if the Commission adopts performance-based rates for cybersecurity incentives, it should neither choose which expenses to approve nor check whether incurred expenses comply with the utility's plans but should simply verify whether predetermined outcomes have been achieved.[291] Ohio FEA recommends that the Commission consider developing resources, such as C2M2, to achieve a performance monitoring tool that will aid in performance-based rates.[292]

c. Commission Determination

159. We interpret the directive to establish 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. This interpretation is consistent with the Commission's finding in Order. No. 679 regarding the directive to establish incentive-based (including performance-based) rate treatments for investments in transmission infrastructure in FPA section 219.[293] Because of the Congressional directive to encourage performance-based rates, the Commission signaled its intention to reevaluate previous Commission policies on performance-based rate treatments and attempt to offer such incentives in the cybersecurity context. We recognize that 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 (*i.e.,* the number and severity of cybersecurity incidents) rather than intermediate steps such as specific cybersecurity protocols or cybersecurity investments that intend to achieve that performance.

160. However, after evaluating the comments, we continue to find that it is difficult to directly observe the success of a cybersecurity investment. We share the view of commenters that it would be premature to adopt generic performance-based rate measures at this time. However, the development of performance-based rate measures may represent a long-term goal for utilities and the Commission to pursue.

D. Cybersecurity Investment Incentive Implementation

1. Cybersecurity ROE Incentive Duration

a. NOPR Proposal

161. The Commission proposed 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) five years from when the cybersecurity investment(s) enter service; [294] (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.[295] The Commission recognized 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. The Commission believed that most cybersecurity incentives granted under this rulemaking would remain in effect

[283] NOPR, 180 FERC ¶ 61,189 at P 44.

[284] *Id.* P 44.

[285] The Commission also explained that, consistent with Order No. 679, which implemented FPA section 219, it interpreted the directive to establish 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. *Id.* P 46 n.41.

[286] *Id.* P 45.

[287] EEI Initial Comments at 12–13; Iowa Utilities Board Initial Comments at 4; Ohio Consumers' Counsel Initial Comments at 14.

[288] EEI Initial Comments at 12.

[289] Ohio Consumers' Counsel Initial Comments at 14.

[290] Iowa Utilities Board Initial Comments at 4.

[291] Ohio FEA Initial Comments at 12.

[292] *Id.* at 12.

[293] Order No 679, 116 FERC ¶ 61,057 at P 270.

[294] For participation in a cybersecurity threat information sharing program, the ''investment'' would recur annually.

[295] NOPR, 180 FERC ¶ 61,189 at P 46.

until the conclusion of the depreciation life of the underlying asset. However, for investments with useful lives exceeding five years, the Commission proposed that the incentive end at the conclusion of five years from the time that the asset receiving the cybersecurity incentive entered service, noting that most IT investments feature useful lives no longer than five years. The Commission preliminarily found that five years is a reasonable expected life to encourage utilities to make an investment and to ensure just and reasonable rates. The Commission also sought comment on whether the proposed duration should be three years instead of five years.

b. Comments

162. EEI comments that the five-year depreciation 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.[296] EEI further comments that, if an incentive becomes mandatory, it is not clear why it must end automatically. EEI argues that, for example, if the investment is in year three and then in year four it becomes a mandatory standard, the utility would lose the incentive moving forward and that this approach will dampen potential incentives to do the work to be an early adopter of promising, qualifying cybersecurity measures.[297] AEP comments that the proposed five-year duration is unlikely to drive utilities to meaningfully reconsider their current and future investment in cybersecurity.[298]

163. APPA, California Parties, the Electricity Consumers Resource Council (ELCON), Ohio Consumers' Counsel, and TAPS state that the Commission should limit the duration proposal to a maximum of three years.[299] California Parties, TAPS, and Ohio Consumers' Counsel argue that setting the limit at three years better aligns with the fast-evolving nature of cybersecurity technology, and that consumers should not have to pay for technology that has become obsolete.[300] APPA comments that, where an asset has a useful life of no more than five years, a three-year Cybersecurity ROE Incentive would apply to a large portion, and potentially all, of the asset's useful life.[301] APPA states that the value of the Cybersecurity ROE Incentive to a utility would decline over time as the underlying asset depreciates and reduces the rate base to which the ROE adder is applied.[302]

c. Commission Determination

164. As discussed in section III.C.1.c., we do not adopt the NOPR's proposed Cybersecurity ROE Incentive. Consequently, we need not address the duration of this incentive.

2. Cybersecurity Regulatory Asset Incentive Duration and Amortization Period

a. NOPR Proposal

165. The Commission proposed to specify that a utility granted the Cybersecurity Regulatory Asset Incentive must amortize the regulatory asset over five years.[303] The Commission stated that this may reflect the generally short-lived nature of cybersecurity activities and corresponds to the depreciation rates for investments described above.[304] The Commission observed that this period generally relates to the expected useful life and associated cost-of-service amortization period of cybersecurity investments.

166. The Commission also proposed to specify that a utility granted the Cybersecurity Regulatory Asset Incentive may defer eligible expenses for up to five years from the date of Commission approval of the incentive.[305] Under this provision, the Commission proposed 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.[306] The Commission preliminarily found that this limit would be appropriate, given the potentially indefinite nature of certain expenses. The Commission stated that such a limit would also reflect that cybersecurity risks and solutions evolve over time and matches the proposed five-year maximum duration of the Cybersecurity ROE Incentive. The Commission preliminarily found 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.

167. However, the Commission proposed to make an exception to this sunsetting provision for eligible cybersecurity threat information sharing programs.[307] The Commission noted that FPA section 219A(c)(2) directs the Commission to provide incentives for *participation* in cybersecurity threat information sharing programs. The Commission preliminarily found that participation in such cybersecurity threat information sharing programs, which provide participants with ongoing updates about active cybersecurity threats and are therefore distinct from other cybersecurity investments that may become obsolete with the passage of time, warrants a different incentive treatment than other investments. Consequently, the Commission proposed that utilities be able to continue deferring these ongoing 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.

b. Comments

168. EEI supports the NOPR proposal to make an exception to the 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.[308] EEI comments that sharing information about the nature of threats can help electric utilities react to and mitigate the threat.[309]

169. EEI requests clarification that the amortization period would be up to five years, but that five years is not the only duration permissible for amortization.[310]

170. TAPS agrees with the Commission's preliminary finding that the five-year limit balances the goals of ratepayer protection with inducing the desired investment.[311] However, TAPS argues that the NOPR unjustifiably proposed to depart from that balance

[296] EEI Initial Comments at 13.

[297] *Id.* at 14.

[298] AEP Initial Comments at 4–5.

[299] APPA Initial Comments at 5; California Parties Initial Comments at 22; ELCON Initial Comments at 4; Ohio Consumers' Counsel Initial Comments at 15; TAPS Initial Comments at 18–19.

[300] California State Parties Initial Comments at 25; Ohio Consumers' Counsel Initial Comments at 15; TAPS Initial Comments at 19.

[301] APPA Initial Comments at 16.

[302] *Id.* at 16.

[303] As noted above, the cybersecurity investment for participation in a cybersecurity threat information sharing program would recur annually.

[304] NOPR, 180 FERC ¶ 61,189 at P 47.

[305] *Id.* P 48.

[306] The Commission proposed 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 Cybersecurity 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; or (2) the cybersecurity investment becoming mandatory.

[307] NOPR, 180 FERC ¶ 61,189 at P 49.

[308] EEI Initial Comments at 14.

[309] *Id.* at 14.

[310] *Id.* at 14.

[311] TAPS Initial Comments at 20–21.

with regard to expenses incurred for eligible cybersecurity threat information sharing programs by allowing a perpetual incentive on those investments.[312] TAPS argues that the Commission should not adopt such an exception for cybersecurity threat information sharing programs, because it gives no consideration of the requirement to protect ratepayers.[313] TAPS states that the NOPR's distinction from other discrete cybersecurity investments that may become obsolete with the passage of time does not support granting a perpetual incentive for cybersecurity threat information sharing programs.[314] TAPS further argues that the fact that participants are provided with ongoing updates after joining such programs is a recurring benefit that likely increases retention, even absent any incentive.[315]

171. California Parties also oppose the NOPR's exception to the sunsetting provision for eligible cybersecurity threat information sharing programs.[316] California Parties state that, once a utility has elected to participate in CRISP and has paid the requisite start-up costs, there is no longer a purpose served by incentive treatment, given that the utility is able to readily recover all ongoing costs of participation (along with the start-up costs) in transmission rates.[317] California Parties argue that, to provide incentives in this circumstance—where they are simply not needed to induce prudent spending on an annual subscription to CRISP and associated staff time—would result in unjust and unreasonable rates.[318]

c. Commission Determination

172. We adopt the NOPR's proposal to add § 35.48(g)(1) to the Commission's regulations, with one modification. As suggested by EEI, we will modify the NOPR proposal to allow, at the request of the utility, the Cybersecurity Regulatory Asset Incentive duration to be *up to* five years. This revision provides flexibility to requesting utilities while maintaining ratepayer protections. A utility granted the Cybersecurity Regulatory Asset Incentive must amortize the regulatory asset for up to five years. Additionally, a utility granted the Cybersecurity Regulatory Asset Incentive may defer eligible expenses for up to five years from the date of Commission approval of the incentive. Consistent with the NOPR proposal, we find that a five-year amortization period balances the Commission's goals of ratepayer protection and providing an appropriate incentive to encourage utilities to improve their cybersecurity posture. To clarify, incentive-eligible, cybersecurity expenses for each of the five years may be included in rate base and amortized for up to five years, essentially creating five tranches of cybersecurity expenses. We also clarify that if and when cybersecurity measures become mandatory, utilities will cease receiving the Cybersecurity Regulatory Asset Incentive for taking such measures.[319] No additional expenses will be converted to regulatory assets and the unamortized portions of regulatory assets must be incurred as expenses in the year when they were converted back to expenses and immediately removed from rate base.

173. We add § 35.48(g)(2) to the Commission's regulations to provide an exception to the five-year duration limit to the incentive-based rate treatment of cybersecurity investments made to participate in a cybersecurity threat information sharing program. We find that the duration exception for participation in eligible cybersecurity threat information sharing programs as proposed in the NOPR is appropriate. As discussed in the body of this rule, the Congressional mandate to incentivize participation indicates that all participants should be eligible to seek cybersecurity incentives for their participation in eligible programs. Therefore, we decline to remove the exception to the sunsetting provision for participation in an eligible cybersecurity threat sharing program.

3. Filing Process

a. NOPR Proposal

174. The Commission proposed 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. As proposed in the NOPR, 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.[320] The Commission proposed to require utilities to provide detail on the expenditures for which they seek incentives and show how the cybersecurity-related expenditures meet the eligibility requirements, as described in more detail below.

175. In addition, the Commission proposed that 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. The Commission stated that, 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 to reflect incentive rate treatment granted pursuant to these proposed regulations. The Commission explained that 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 and not unduly discriminatory or preferential.[321]

176. The Commission proposed that 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.[322]

177. The Commission also proposed that 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.[323] The Commission alternatively proposed that a utility requesting the Cybersecurity 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.

178. The Commission preliminarily found that the same cybersecurity investment should not be eligible for both the Cybersecurity ROE Incentive and the Cybersecurity Regulatory Asset Incentive. Given that regulatory asset treatment may be approved for costs that are normally treated as expenses (*i.e.,* as regulatory assets), the Commission preliminarily 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

[312] *Id.* at 21.
[313] *Id.* at 21.
[314] *Id.* at 22.
[315] *Id.* at 22.
[316] California Parties Initial Comments at 27.
[317] *Id.* at 27.
[318] *Id.* at 27.
[319] *See Cal. Pub. Util. Comm'n* v. *FERC,* 879 F.3d 966 (9th Cir. 2018).
[320] NOPR, 180 FERC ¶ 61,189 at P 50.
[321] *Id.* P 51 & n.47.
[322] *Id.* P 52.
[323] *Id.* P 53.

associated with the 200-basis point ROE adder.[324]

b. Comments

179. Ohio Consumers' Counsel requests that the Commission require any incentive application (whether an application for incentives for advanced technologies and actions on the pre-qualification list or for incentives that are not included on that list) to be made in a FPA section 205 filing.[325] Ohio Consumers' Counsel further requests that the Commission require that both types of applications explicitly identify in which accounts the utility will book the costs associated with the investment, expense or action.[326] Ohio Consumers' Counsel comments that such a requirement is needed to ensure transparency and proper rate treatment for these investments.[327]

180. California Parties ask the Commission to clarify the incentive application procedures to ensure that stakeholders have adequate time and information to meaningfully review and comment on incentive requests.[328] California Parties argue that the usual filing procedures under FPA section 205 are not sufficient because they neither provide ample time for review, given the more complex nature of cybersecurity incentive applications, nor do the procedures ensure the development of an adequate factual record, especially given the CEII considerations.[329] In support, California Parties state that the filing procedures under FPA section 205 provide only 21 days for an interested party to intervene and comment and do not ensure the opportunity for discovery or evidentiary hearings.[330] California Parties request that the Commission make clear that all cybersecurity incentive applications will be presumed to raise issues of material fact and will thus be subject to an evidentiary hearing with an opportunity for discovery.[331] California Parties aver that evidentiary hearings and discovery would provide a critical measure of transparency regarding the use of ratepayer funds, provided appropriate safeguards are in place.[332]

181. NRECA seeks additional detail on the NOPR's proposed filing process.[333] Specifically, NRECA requests that the Commission propose language addressing applications under the case-by-case approach.[334] NRECA also asks the Commission to describe the anticipated composition of teams responsible for reviewing and evaluating requests under the proposed new provisions.[335] NRECA states that, given the wide-ranging implications of granting cybersecurity incentives, the reviewing team should include staff with diverse backgrounds, including electrical engineers who understand the structure of the transmission and generations assets that may be affected by the proposed cybersecurity investment, system or computer science engineers who understand the nature of the proposed investments, and analysts with ratemaking experience who can balance the increased benefits of the proposed investment against the cost to the ratepayers.[336]

182. MISO Transmission Owners caution that, while the inclusion of cybersecurity threat information sharing programs on the PQ List will provide certainty, efficiency, and transparency for utilities seeking an incentive, public disclosure through the filing process could put utilities at risk.[337] MISO Transmission Owners recommend that the Commission adopt filing procedures that would protect the confidentiality of utilities requesting incentives, including the use of a public cover sheet disclosing what incentives are being applied for with the remainder of the application being confidential.[338] In contrast, NRECA acknowledges the need for utilities to submit certain information under CEII filing regulations but warns that the more information filing utilities are able to hide from the public, the greater the burden on interested parties.[339] NRECA cautions that the consolidation of incentive applications containing sensitive information may increase the overall risk to the bulk electric system.[340]

c. Commission Determination

183. We adopt the NOPR's proposal and add § 35.48(h) to the Commission's regulations, which specifies the details required in applications to the Commission to receive incentive-based rate treatment for cybersecurity investments. We clarify that utilities may request Commission approval of incentives for cybersecurity investments pursuant to FPA section 219A by filing an FPA section 205 filing or by seeking a ruling on eligibility by filing a petition for declaratory order followed-up by an FPA section 205 filing. Utilities must propose to revise their rates to reflect such incentives pursuant to FPA section 205. Pursuant to FPA section 219A(f), § 35.48(h) permits utilities to seek cybersecurity incentives either as part of a larger rate case or make a request for single issue ratemaking.[341]

184. With regard to Ohio Consumers' Counsel's suggestion that the Commission require any incentive application (whether an application for incentives for Advanced Cybersecurity Technologies and actions on the PQ List or for incentives that are not included on that list) to be made in a FPA section 205 filing, we agree that an FPA section 205 filing is necessary for any incentives to be effectuated in utility rates. However, consistent with the Commission's precedent with respect to transmission incentives, we will allow utilities to seek declaratory orders finding expenditures to be eligible for incentives prior to making FPA section 205 filings to implement incentives in rates. A request for a declaratory order must include all necessary information for the Commission to determine whether the investment merits an incentive. The FPA section 205 filing necessary to add incentive-based rate treatment to a utility's rate on file with the Commission, whether filed in conjunction with a petition for declaratory order or on its own, must provide information required for the Commission to determine that the rate inclusive of the incentives is just and reasonable and not unduly discriminatory or preferential.[342]

185. The filing process is similar for incentives requested for cybersecurity investments that are on the PQ List and case-by-case requests. The distinction is that requests for incentives for cybersecurity investments that are on the PQ List have the rebuttable presumption that the items on the PQ List satisfy the eligibility criteria, *i.e.,* materially improving cybersecurity posture and not already being mandatory. By contrast, applicants under a case-by-case approach must provide a detailed description of how the cybersecurity investments will satisfy the eligibility criteria and thereby materially improve the cybersecurity posture for their utility. To make this demonstration, in addition to describing

[324] *Id.* P 38.

[325] Ohio Consumers' Counsel Initial Comments at 9.

[326] *Id.* at 9–10.

[327] *Id.* at 10.

[328] California Parties Initial Comments at 30.

[329] *Id.* at 30.

[330] *Id.* at 30.

[331] *Id.* at 31.

[332] *Id.* at 31.

[333] NRECA Initial Comments at 10–12.

[334] *Id.* at 11.

[335] *Id.* at 11.

[336] *Id.* at 11–12.

[337] MISO Transmission Owners Initial Comments at 7.

[338] *Id.*

[339] NRECA Initial Comments at 13.

[340] *Id.* at 13.

[341] IIJA, Public Law 117–58, section 40123, 135 Stat. at 952 (to be codified at 16 U.S.C. 824s–1(f)).

[342] 18 CFR pt. 35.

the cybersecurity investments, applicants should: (1) describe their prevailing cybersecurity posture including existing equipment, processes, and ongoing expenses; and (2) describe how the cybersecurity investment for which an incentive is sought would elevate the utility's cybersecurity posture. The application should include evidence sufficient to demonstrate that the cybersecurity investment(s) would be for activities that are consistent with the discussion in section III.B. regarding the PQ List and case-by-case approaches. We also clarify that, for incentive requests either for PQ List items or on a case-by-case basis, utilities must include in their transmittal letter an attestation that, to their knowledge, the cybersecurity investments are not mandatory, as described in section III.A.3. above. Additionally, for the Cybersecurity Regulatory Asset Incentive, the transmittal letter must include an attestation that the utility has not already been undertaking materially the same cybersecurity expenses for more than three months (with the exception of participation in cybersecurity threat information sharing programs).[343] As described in III.C.2. only new types of cybersecurity investments, and not materially similar ones to existing expenses, will be eligible for incentive-based rate treatment.

186. As described in § 35.48(h), requests for the Cybersecurity Regulatory Asset Incentive must provide: (1) a description of the relevant cybersecurity expenses; (2) estimates of the costs of cybersecurity expenses; (3) a description of when the cybersecurity expenses are expected to be incurred; and (4) an attestation that the utility's cybersecurity expenses are new, *i.e.,* the utility has not already been undertaking materially the same cybersecurity expenses for more than three months prior to the date of filing its request with the Commission. Descriptions of expenses should include details such as whether they are conducted by utility employees or third parties and whether they are for training or the direct carrying out of cybersecurity tasks. This last requirement seeks to ensure that cybersecurity incentives encourage utilities to improve their cybersecurity posture rather than provide a return on expenses that the utility is already undertaking. Incentive-eligible expenses should be meaningfully distinct from past ones and not only contain small variations or incremental modifications from existing expenses.

187. Consistent with the Commission's implementation of transmission incentives under FPA section 219, interested parties will have a 21-day comment period, unless otherwise provided by the Commission.[344] We find that California Parties have not justified departing from the Commission's comment period convention. Doing so could impede the timeliness of the Commission's evaluation of cybersecurity incentives. Furthermore, we will not presume that every request for cybersecurity incentives will have issues of material fact requiring hearing and settlement judge procedures. Such a presumption would also constitute an unjustified departure from Commission incentive precedent under FPA section 219 and may unnecessarily delay the incentive-based rate treatment of cybersecurity investments as well as the utility's underlying cybersecurity investments.

188. In response to Ohio Consumers' Council suggested requirement that utilities identify the accounts that cybersecurity investment will be booked in, as described in section III.C.2, pursuant to our existing regulations, any utility that receives an incentive must maintain sufficient records to support the distinction of any investments that are afforded incentive-based rate treatment.

189. We will not, as NRECA suggests, describe the anticipated composition of Commission staff responsible for reviewing and evaluating requests under the proposed new provisions. Such description is neither necessary nor consistent with Commission procedures.

190. Consequently, for a given cybersecurity investment, utilities will be able to receive a single incentive-based rate treatment, as discussed in section III.B., for each voluntary cybersecurity investment that the utility makes. Utilities must specify which incentive they seek in their filings with the Commission.

191. We note that § 35.48(j) to the Commission's regulations declares that utilities may request CEII treatment pursuant to § 35.48(k) to the Commission's regulations for the portions of their cybersecurity incentive-based rate filings that contains CEII. This is consistent with § 388.113 of the Commission's regulations.[345] In addition, FPA section 219A(g) declares that Advanced Cybersecurity Technology Information provided to the Commission under FPA 219A(b), (c), or (f) ''shall be considered to be Critical Electric Infrastructure Information under [FPA] section 215A.'' [346]

4. Reporting Requirements

a. NOPR Proposal

192. 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, the Commission proposed to require utilities to submit informational reports to the Commission for the duration of the incentive.[347]

193. The Commission also proposed that 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.[348] 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. The Commission proposed that 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, the Commission proposed that 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 Cybersecurity Regulatory Asset Incentive, the Commission proposed that 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.

194. The Commission noted that it could also conduct periodic verification to assess cybersecurity investments and expenses for which it has approved

[343] For ongoing cybersecurity investments made to comply with approved Reliability Standards, the three-month period begins on the date that the Commission's approval of the Reliability Standard becomes effective. For approvals that the Commission issues by order, the effective date is the date of the order. For approvals that the Commission issues by rulemaking, the effective date occurs on a specified date that occurs after the later of Congress receiving notice from the Commission or the final rule is published in the **Federal Register**.

[344] 18 CFR 35.8.

[345] 18 CFR 388.113.

[346] IIJA, Public Law 117–58, section 40123, 135 Stat. at 951 (to be codified at 16 U.S.C. 824s–1(g)).

[347] NOPR, 180 FERC ¶ 61,189 at P 54.

[348] *Id.* P 55.

incentives.[349] The Commission could perform such verifications through multiple means (*i.e.,* directing further informational filings, audits, etc.). The Commission stated that the annual informational filings would inform the Commission on how and when any additional verification is warranted.

b. Comments

195. Ohio Consumers' Counsel supports the NOPR's proposal and recommends that the Commission and consumers must both be able to verify that the investments are being made and that the intended benefits are being received.[350]

196. Several commenters ask for the Commission to require additional information beyond the proposed reporting requirements. NRECA requests that the Commission require that the annual informational filings include any changes to the categorization of any incentivized enhancements and affirmatively state that the previously incentivized enhancement remains valid.[351] NRECA states that this modification will address the burden placed on ratepayers to review and analyze the information provided to ensure the accuracy of formulas applying different ROEs, especially where certain of those ROEs are capped.[352] NRECA also asks that the Commission consider issuing responses confirming the continued applicability of incentive rate treatment in response to the annual informational filings.[353] Ohio FEA recommends that verification methods should be established that go beyond the annual information filings proposed by the NOPR to ensure that cybersecurity benefits are realized and that double recovery of incentives is avoided.[354] NRECA also recommends that the Commission establish a process to confirm whether a utility's cybersecurity investment had the security effects described.[355]

197. California Parties urge the Commission to require utilities awarded cybersecurity incentives to submit aggregated data and, consistent with the Commission's CEII regulations, provide vetted State officials access to it.[356] California Parties argue that the provision of such data will, in turn, enable the relevant State officials to improve the cybersecurity protection of utility assets in their respective states.[357]

198. While not opposed to the NOPR proposal, EEI states that the Commission should 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.[358] EEI states that, given the sensitivity of information filed as part of an annual report, electric companies would need assurances regarding how the various 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.[359]

c. Commission Determination

199. Consistent with the NOPR, in order to ensure that a utility receiving incentive-based rate treatment has implemented and continues to adhere to the requirements of the incentive, we require utilities to submit informational reports to the Commission for the duration of the cybersecurity incentive, pursuant to § 35.48(i), which we are adding to the Commission's regulations. We continue to find that cybersecurity investments, unlike many others, may not otherwise be observable and verifiable by other parties. Consistent with the comments of Ohio Consumers' Counsel and California Parties, this requirement should provide State commissions and other stakeholders enhanced visibility into the cybersecurity investments that utilities are making for which they receive incentives.

200. Consistent with the NOPR, a utility that has received cybersecurity incentives under this section must make an annual informational filing by June 1 of that calendar year, 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 within 60 days before June 1 must submit an annual informational filing beginning on June 1 of the following year.[360] The annual filing must 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 the cybersecurity investments are booked. For recipients of the Cybersecurity Regulatory Asset Incentive, annual informational filings should describe expenses in sufficient detail to demonstrate that such expenses specifically relate to the eligible cybersecurity investment and not to ongoing services including system maintenance, surveillance, and other labor costs that are materially the same as those that existed prior to the incentive request. Additionally, consistent with NRECA's comments, annual informational filings must specify any material changes in the nature of such expenses from prior filings. Unlike capital investments, ongoing expenses could potentially change in nature over time, and this provision ensures that the incentives in utility rates correspond to the precise expenses for which the Commission approved incentives.

201. We will not, as requested by NRECA, include a requirement for the Commission to issue responses confirming the continued applicability of incentive rate treatment in response to the annual informational filings. We do not find that such affirmative confirmation is necessary to ensure that incentives continue to be just and reasonable.

202. We also decline to establish a process to confirm whether a utility's cybersecurity investment had the security effects described as recommended by NRECA.[361] The annual informational filings will enable the Commission and interested parties to confirm that utilities have made the cybersecurity investments for which they receive incentives. Establishing a process to review the efficacy of each cybersecurity investment would create a substantial regulatory burden on utilities and other parties, including the Commission. Furthermore, measuring the ultimate effect of specific cybersecurity investments may be difficult given that security defenses can act as a deterrence to cyberattack and therefore it is impossible to know what cyberattacks have been prevented.

203. We note that § 35.48(j) to the Commission's regulations declares that utilities may request CEII treatment pursuant to § 35.48(i) to the Commission's regulations for the portions of their cybersecurity incentive-based rate informational reports that contain CEII. This is consistent with § 388.113 of the

[349] *Id.* P 56.

[350] Ohio Consumers' Counsel Initial Comments at 16.

[351] NRECA Initial Comments at 12.

[352] *Id.* at 12.

[353] *Id.* at 12.

[354] Ohio FEA Initial Comments at 13.

[355] NRECA Initial Comments at 9.

[356] California Parties Initial Comments at 34.

[357] *Id.* at 34–35.

[358] EEI Initial Comments at 16.

[359] *Id.* at 17.

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

[361] NRECA Initial Comments at 9.

Commission's regulations.[362] In addition, FPA section 219A(g) declares that Advanced Cybersecurity Technology Information provided to the Commission under FPA 219A(b), (c), or (f) ''shall be considered to be Critical Electric Infrastructure Information under [FPA] section 215A.'' [363]

E. Other Issues

1. Comments

204. INGAA and the International Pipeline Resilience Organization (IPRO) support the Commission's efforts to provide cybersecurity incentives to electric utilities but argue that rate-based incentives should also be available to owners and operators of interstate natural gas pipelines under the Commission's authority.[364] Both commenters assert that, due to the highly interconnected nature of the electric and gas industries and the similarities in threats faced by both industries, the Commission is overlooking a security threat by solely focusing on incentives for electric utilities.[365] IPRO argues that the Commission has the requisite authority under the NGA and the Interstate Commerce Act (ICA) to offer incentives to the oil and gas industry.[366] In contrast, California Parties assert that, because the NOPR does not cite the NGA or ICA, the Commission cannot include incentives for pipeline owners and operators in the final rule.[367]

205. EPSA urges the Commission to prevent cross-subsidization among vertically integrated entities. EPSA avers that, while these companies may have separate legal entities for their transmission and generation operations, cybersecurity programs are often administered as a shared service. EPSA argues that the Commission must ensure that any entities to which it extends incentives on the transmission side are not cross-subsidizing cybersecurity operations for their generation arms.[368]

2. Commission Determination

206. We will not, as IPRO advocates, extend incentives to natural gas pipelines and oil pipelines in this proceeding. This rulemaking effectuates Congress' requirement that the Commission develop cybersecurity incentives for utilities pursuant to FPA section 219A. As noted by California Parties, incentives under the NGA and the ICA are beyond the scope of this proceeding. We also note that the application of longstanding cost-of-service cost-allocation practices to enterprise-wide costs, described in sections III.C.1 and III.C.2 above, will address EPSA's cross-subsidization concerns.

IV. Information Collection Statement

207. The information collection requirements contained in this final rule 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.[369] 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 final rule establishes the Commission's regulations with respect to the implementation of FPA section 219A.[370]

208. 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).

209. The Commission solicited comments on the NOPR and the collection of information in that NOPR.

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

Action: Proposed revision of FERC–725B.

OMB Control No.: 1902–0248.

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

Frequency of Information Collection:

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

Annually: An informational filing on June 1 of each year, required of entities that have been granted and are receiving incentive-based rate treatment for cybersecurity expenditures.

Abstract: The final rule provides 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 final rule 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 final rule refers to this list of pre-qualified expenditures that are eligible for incentives as the PQ List. Any cybersecurity expenditure that is on the PQ List is entitled to a rebuttable presumption of eligibility for an incentive.

210. The final rule also discusses a different 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 and not unduly discriminatory or preferential.

211. The final rule also provides 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.

Necessity of Information: Required to obtain or retain benefits.

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

[362] 18 CFR 388.113.

[363] IIJA, Public Law 117–58, section 40123, 135 Stat. at 951 (to be codified at 16 U.S.C. 824s–1(g)).

[364] INGAA Initial Comments at 2; IPRO Initial Comments at 2–3.

[365] INGAA Initial Comments at 2; IPRO Initial Comments at 2–3.

[366] IPRO Initial Comments at 9–10.

[367] California Parties Reply Comments at 14.

[368] EPSA Initial Comments at 9.

[369] 5 CFR 1320.11.

[370] Public Law 117–55, 135 Stat. 951 (2021) (to be codified at 16 U.S.C. 824s–1).

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.

212. 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 [371] and cost [372] as follows:

FERC–725B—CHANGES IN FINAL RULE 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 × Column C)	E. Average burden hours & cost ($) per response	F. Total estimated burden hours & total estimated cost ($)(Column D × Column E)
Voluntary filing seeking incentive rate treatment for cybersecurity investment. 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. 18 CFR 35.48(h).	50	1	50	40 hours; $3,640 ...	2,000 hours; $182,000
Totals	.....	.....	.....	.....	6,000 hours; $546,000

V. Environmental Analysis

213. 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.[373] We conclude that that neither an Environmental Assessment nor an Environmental Impact Statement is required for this final rule under § 380.4(a)(15) of the Commission's regulations, which provides a categorical exemption for approval of actions under sections 205 and 206 of the FPA relating to the filing of schedules containing all rates and charges for the transmission or sale of electric energy subject to the Commission's jurisdiction, plus the classification, practices, contracts, and regulations that affect rates, charges, classifications, and services.[374]

VI. Regulatory Flexibility Act

214. The Regulatory Flexibility Act of 1980 (RFA) [375] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[376] The SBA size standard for electric utilities is based on the number of employees, ranging from 250 to 1,000 employees based on the electric utility type.[377] While this final rule is applicable to all small utilities, participation with this final rule is voluntary for all respondents, including small utilities. We estimate that the average cost of voluntary participation for each utility to be $7,280 (initial filing) plus an annual estimated cost of $3,640 for up to five years. These initial and annual estimated costs would not constitute a significant economic impact on affected entities of any size, including small entities. Accordingly, the Commission certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

VII. Document Availability

215. In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the internet through the Commission's Home Page (*http://www.ferc.gov*). At this time, the Commission has suspended access to the Commission's Public Reference Room due to the President's March 13, 2020 proclamation declaring a National Emergency concerning the Novel Coronavirus Disease (COVID–19).

216. From FERC'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 document in the docket number field.

217. User assistance is available for eLibrary and the FERC's website during normal business hours from FERC 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. Email the Public Reference Room at *public.referenceroom@ferc.gov.*

VIII. Effective Date and Congressional Notification

218. These regulations are effective [insert date 60 days from publication in **Federal Register**]. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a ''major rule'' as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

List of Subjects in 18 CFR Part 35

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

[371] ''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.

[372] 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.

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

[374] 18 CFR 380.4(a)(15).

[375] 5 U.S.C. 601–612.

[376] 13 CFR 121.101.

[377] 13 CFR 121.201.

By the Commission. Commissioner Danly is dissenting with a separate statement attached.

Issued: April 21, 2023.

Debbie-Anne A. Reese,

Deputy Secretary.

In consideration of the foregoing, the Commission hereby amends 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 with rates on file with the Commission that voluntarily make cybersecurity investments as described in this section.

(b) *Definitions.* As used in this section:

Advanced Cybersecurity Technology means 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 (as defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)).

Advanced Cybersecurity Technology Information means information relating to Advanced Cybersecurity Technology or proposed Advanced Cybersecurity Technology that is generated by or provided to the Commission or another Federal agency. Pursuant to FPA section 219A(g), Advanced Cybersecurity Technology Information is considered to be Critical Electric Infrastructure Information.

Critical Energy/Electric Infrastructure Information (CEII) has the same meaning as defined in 18 CFR 388.113.

Electric Reliability Organization has the same meaning as defined in § 39.1 of this subchapter.

Reliability Standard has the same meaning as defined in § 39.1 of this subchapter.

(c) *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, provided that the utility meets the requirements of this section and the utility demonstrates that the resulting rate is just and reasonable and not unduly discriminatory or preferential, as required by sections 205 and 206 of the Federal Power Act. 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 a single incentive-based rate treatment as specified in paragraph (f) of this section for an eligible cybersecurity investment that meets the eligibility criteria set forth in paragraph (d) of this section.

(d) *Eligibility criteria.* Pursuant to paragraphs (e) through (k) of this section, a utility may receive incentive-based rate treatment for a cybersecurity investment that:

(1) Materially improves cybersecurity through either Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program; and

(2) Is not already mandated by the Reliability Standards as maintained by the Electric Reliability Organization, or otherwise mandated by local, State, or Federal law, decision, or directive; otherwise legally mandated; or an action taken in response to a Federal or State agency merger condition, consent decree from Federal or State agency, or settlement agreement that resolves a dispute between a utility and a public or private party.

(e) *Demonstrating satisfaction of the eligibility criteria.* A utility shall demonstrate to the Commission that a proposed cybersecurity investment satisfies the eligibility criteria in paragraph (d) of this section. Such demonstration shall show that the cybersecurity investment fulfills at least one of the provisions in the following paragraphs (e)(1) through (3):

(1) A utility shall demonstrate that a cybersecurity investment qualifies as one or more of the pre-qualified cybersecurity investments. The Commission shall rebuttably presume that pre-qualified cybersecurity investments satisfy the eligibility criteria. The Commission shall maintain a list on its website of pre-qualified cybersecurity investments and shall update such list from time to time either subject to notice and comment procedures or in a rulemaking.

(2) A utility shall demonstrate that a cybersecurity investment satisfies each of the eligibility criteria in paragraph (d) of this section. The Commission shall not presume that such demonstration satisfies the eligibility criteria.

(3) A utility shall demonstrate that it will make cybersecurity investments to comply with a Reliability Standard that is approved by the Commission but has not yet taken effect as approved by the Commission. The Commission shall not presume that such demonstration satisfies the eligibility criteria. Any incentives authorized by the Commission pursuant to this section shall terminate when the Reliability Standard takes effect.

(f) *Types of incentive-based rate treatment for cybersecurity investment.* For purposes of this section, incentive-based rate treatment shall mean deferral of expenses as a regulatory asset.

(g) *Incentive duration.* (1) A deferred Advanced Cybersecurity Technology regulatory asset whose costs are typically expensed shall be:

(i) Amortized over a period of up to five years;

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

(iii) Limited to ongoing expenses that the applicable utility was not already undertaking more than three months prior to filing an incentive request; and

(iv) Terminated when the cybersecurity investment or activity that serves as the basis of that incentive becomes mandatory.

(2) An incentive granted for participation in a qualified cybersecurity threat information sharing program will not be subject to the five-year duration limitation provisions of paragraph (g)(1)(ii) of this section for as long as the utility participates in the qualified cybersecurity threat information sharing program and such participation is not mandatory as to the utility. A utility participating in a qualified cybersecurity threat information sharing program is eligible to continue deferring expenses associated with such participation, which for each year would be amortized over the next five years.

(h) *Incentive applications.* For the purpose of this section, a utility's request for incentive based-rate treatments for one or more cybersecurity investments must be made in a filing pursuant to section 205 of the Federal Power Act, or in a petition for a declaratory order that precedes a filing pursuant to section 205 of the Federal Power Act. Utilities may file such a request either as a part of a general rate request or on a single-issue basis. Such a request shall include a detailed explanation to include the following information:

(1) A demonstration that the cybersecurity investment satisfies the eligibility criteria, which includes an attestation that cybersecurity investment is not mandatory, as required by paragraph (d)(2) of this section, and that the resulting rate is just and reasonable and not unduly discriminatory or preferential; and

(2) A detailed description of relevant cybersecurity expenses, including whether such cybersecurity expenses are:

(i) Associated with third-party provision of hardware, software, computing networking services, and/or cybersecurity monitoring services;

(ii) For training to implement network analysis and monitoring programs, and/or other cybersecurity protocols; and/or

(iii) Other cybersecurity expenses;

(3) Estimates of the cost of such cybersecurity expenses;

(4) When the cybersecurity expenses are expected to be incurred; and

(5) An attestation that the utility either has not already been undertaking duplicative or materially the same expenses for more than three months or that the utility is participating in a cybersecurity threat information-sharing program for the expense at issue. In the case of cybersecurity investments made to comply with a Reliability Standard that is approved by the Commission but has not yet taken effect as approved by the Commission pursuant to paragraph (e)(3) of this section, the utility must attest that it has not already been undertaking duplicative or materially the same expenses for more than three months prior to the date that the Commission's approval of the Reliability Standard becomes effective.

(i) *Reporting requirements.* A utility that has received Commission approval for incentive-based rate treatment under this section shall make an annual informational filing on June 1, provided that the utility has received such Commission approval at least 60 days prior to June 1 of that year. A utility that receives Commission approval of an incentive-based rate treatment under this section later than 60 days prior to June 1 shall submit an annual informational filing beginning on June 1 of the following year. The annual filing shall detail the specific cybersecurity investments that were made pursuant to the Commission's approval and the corresponding FERC account used. The annual informational filing shall describe the deferred 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. Utilities shall provide a detailed description of any material changes in the nature of such expenses from prior year informational filings.

(j) *Transmittal of CEII in incentive applications and annual reports.* As appropriate, any CEII submitted to the Commission in a utility's incentive application made pursuant to paragraph (k) of this section or contained in its reporting requirements made pursuant to paragraph (i) of this section shall be filed consistent with 18 CFR part 388.

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

UNITED STATES OF AMERICA

Incentives for Advanced Cybersecurity Investment, Docket No. RM22–19–000

DANLY, Commissioner, *dissenting:*

1. I dissent from today's Final Rule [378] because it is not in line with the Infrastructure Investment and Jobs Act (IIJA) directive to establish incentive-based rate treatments that ''encourag[e]'' ''investments by public utilities in advanced cybersecurity technology'' and ''participation by public utilities in cybersecurity threat information sharing programs.'' [379] Some have stated that Congress intended for the IIJA to ''shore up cybersecurity'' across the energy sector and other critical infrastructure.[380] The Final Rule provides cybersecurity incentives to select energy sector participants and only a few cybersecurity investments. This rule does not ''shore up cybersecurity'' of the bulk power system. At best, it is a tepid response to a clear Congressional mandate.

2. *First,* the Final Rule limits incentives and cost recovery to those public and non-public utilities ''that have or will have a [cost-based] rate [tariff] on file with the Commission.'' [381] Put differently, the Final Rule excludes public and non-public utilities that sell electricity at market-based rates. This exclusion is not narrow. In 2019, the Commission estimated that there were over 2,500 market-based rate sellers.[382]

3. Given the size of the population excluded, one would expect the IIJA to have directed such limitation. It does not. The statute directs the Commission to establish incentive-based rate treatments that ''encourage'' ''public utilities'' to make cybersecurity investments and participate in cybersecurity information sharing programs. It allows for single-issue rate filings and does not distinguish between those utilities with cost-of-service rates from those with market-based rates.

4. Nor does the broader context of the IIJA support such exclusion.[383] A reading of the IIJA's cybersecurity provisions in their entirety make evident that Congress intended for agencies to immediately undertake a broad campaign to support cybersecurity investment in the energy sector. The IIJA directed the Commission to establish cybersecurity incentives within 1.5 years of its enactment.[384] Further, as noted by the Electric Power Supply Association (EPSA), ''Congress specifically cites small or medium-sized public utilities with limited cybersecurity resources as being potentially eligible for *additional* incentives beyond those identified in the legislation, demonstrating the Congressional intent to fortify the entirety of the [Bulk Power System] to the greatest extent that is reasonably possible.'' [385] The IIJA also directed the Secretary of Energy to ''*enhance*[ ] grid security,'' [386] ''*deploy* advanced cybersecurity technologies for electric utility systems,'' [387] and ''*increase* the

[378] *Incentives for Advanced Cybersecurity Investment,* 183 FERC ¶ 61,033 (2023) (Final Rule).

[379] Public Law 117–58, section 40123(c), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(c)).

[380] *See, e.g.,* Senate Committee on Energy & Natural Resources, Chairman Manchin Opening Remarks, at 6 (Mar. 23, 2023), *https://www.energy.senate.gov/services/files/3D1ABB79-6CBF-4786-872A-E708A87CB6AB* (''We took action last Congress by providing $1.9 billion in the Infrastructure Investment and Jobs Act to shore up cybersecurity across the transportation, energy, and water sectors by supporting utilities and State and local governments. I am immensely proud of this work.'').

[381] Final Rule, 183 FERC ¶ 61,033 at P 23 (citation omitted).

[382] *Data Collection for Analytics & Surveillance & Market-Based Rate Purposes,* Order No. 860, 168 FERC ¶ 61,039, at P 324 (2019).

[383] *See McCarthy* v. *Bronson,* 500 U.S. 136, 139 (1991) (''[S]tatutory language must always be read in its proper context.''); *Crandon* v. *U.S.,* 494 U.S. 152, 158 (1990) (''In determining the meaning of the statute, we look not only to the particular statutory language, but to the design of the statute as a whole and to its object and policy.'') (citations omitted).

[384] Public Law 117–58, section 40123(b)–(c), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(b)–(c)) (requiring the Commission to conduct a study to identify incentive-based rate treatments within 180 days after the enactment of the section and establish a rule for incentive-based rate treatment within one year thereafter).

[385] EPSA, November 7, 2022 Comments, at 6 (Accession No. 20221107–5130) (emphasis in original) (EPSA Comments). The IIJA also authorized the Commission to provide ''additional incentives'' if that ''investment in advanced cybersecurity technology or information sharing program costs will reduce cybersecurity risks to . . . defense critical electric infrastructure.'' Public Law 117–58, section 40123(d), 135 Stat. 429, 952 (codified at 16 U.S.C. 824s–1(d)).

[386] *Id.,* section 40121, 135 Stat. 429, 949 (emphasis added).

[387] *Id.,* section 40124(c), 135 Stat. 429, 954 (emphasis added).

participation of eligible entities in cybersecurity threat information sharing programs.'' [388] Simply put, excluding 2,500 market-based rate sellers from cybersecurity incentives and cost recovery is not in line with Congressional intent. It should also not go unnoticed that the majority fails to include the provisions from the IIJA in its revised regulations regarding additional incentives for certain utilities, including defense critical electric infrastructure and small and medium utilities,[389] without any explanation although there really can be none.

5. What Congress intended is of no consequence to the majority. On top of failing to respond meaningfully to EPSA's argument regarding Congressional intent (an Administrative Procedure Act violation),[390] my colleagues declare (without citing to any provision in the IIJA) that ''utilities that make sales of energy, capacity, or ancillary services at market-based rates should [not] be able to continue to make those sales and also separately recover the costs of, and receive incentive-based rate treatment on, eligible cybersecurity investments.'' [391] Then the majority goes on to claim that the ''final rule meets the requirements of [the IIJA]'' because ''[a]ll sellers of energy, capacity, and ancillary services are free to file cost-of-service rates under FPA section 205 . . . to recover their entire cost of service'' and ''proceed to make sales exclusively under that cost-based rate.'' [392] In other words, the Commission has fulfilled the Congressional mandate because 2,500 market-based rate sellers can always abandon their market-based rate authority and make filings to transact only at cost-based rates.

6. That reasoning is untenable. The IIJA intended agencies to adopt policies and rules that would induce swift and efficient investments in cybersecurity by the entire energy sector—it was not designed to undermine competitive markets. Moreover, the majority's interpretation effectively voids the IIJA's directive that ''[t]he Commission *shall permit* public utilities to apply for incentive-based rate treatment under a rule issued under this section on a single-issue basis by submitting to the Commission a tariff schedule under [FPA] section [205 [393]] . . . that permits recovery of costs and incentives over the depreciable life of the applicable assets, without regard to changes in receipts or other costs of the public utility.'' [394]

7. Public utilities submit revisions both to market-based rate tariffs and cost-based rate tariffs under FPA section 205. While the proposed rule stated that utilities must file to recover costs and incentives in accordance with FPA section 205 and identified certain filing requirements as to utilities with formula rates and stated rates,[395] at no time did the Commission suggest that entities currently making sales of energy, capacity and ancillary services under market-based rate tariffs must make a filing to recover their *entire* cost of service, including costs of and an incentive return on, cybersecurity investments and proceed to make sales *exclusively* under that cost-based rate, as set forth in the final rule. The final rule is not a ''logical outgrowth'' [396] of the proposed rule, and its sharp departure from the proposed rule violates that the Administrative Procedure Act (APA) requirement that agencies engaged in a rulemaking must provide interested parties adequate notice and opportunity to comment on a proposed rule.[397] It also is nonsensical. Even under the construct today, a generation utility may have both a market-based rate tariff under which it sells energy, capacity and ancillary services and a cost-based rate tariff under which it recovers a reactive power revenue requirement. There is no requirement that such generation utility abandon its market-based rate tariff to recover its cost-based rates. Because the proposed rule failed to provide adequate notice to the public of any change as to market-based rate sellers, this violation of the APA is an obvious legal error.

8. *Second,* the Final Rule unilaterally imposes the heightened requirement that each ''cybersecurity investment[s] [must] . . . *materially improve* cybersecurity through either an investment in Advanced Cybersecurity Technology or participation in a cybersecurity threat information sharing program.'' [398] The IIJA includes no such materiality requirement. Congress directed the Commission to ''encourage[ ]—(1) investments by public utilities in advanced cybersecurity technology; and (2) participation by public utilities in cybersecurity threat information sharing programs.'' [399]

9. The IIJA already limits what qualifies as ''advanced cybersecurity technology'' to ''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.'' [400] The ordinary meaning of ''enhance'' is ''to improve the quality, amount, or strength of something.'' [401] It is not to ''materially improve the quality, amount or strength of something.''

10. While the IIJA does not explicitly define ''cybersecurity threat information sharing program,'' [402] it can be inferred that the statute requires (1) that there is a ''program,'' (2) that ''information [is] shar[ed],'' and (3) that information relates to ''cybersecurity.'' The statute cannot be read as inferring a requirement that the utility's participation must ''materially improve'' the security posture of that utility. The additional requirements in the Final Rule that the information be ''relevant and actionable'' and program be ''sponsored by the federal or state government'' are arbitrary and subjective and also is not in line with

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

[389] *See id.,* section 40123(d), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(d)).

[390] *See TransCanada Power Mktg. Ltd.* v. *FERC,* 811 F.3d 1, 12 (D.C. Cir. 2015) (''It is well established that the Commission must 'respond meaningfully to the arguments raised before it.''') (quoting *Pub. Serv. Comm'n* v. *FERC,* 397 F.3d 1004, 1008 (D.C. Cir. 2005)).

[391] Final Rule, 183 FERC ¶ 61,033 at P 26.

[392] *Id.* (citation omitted).

[393] 16 U.S.C. 824d.

[394] Public Law 117–58, section 40123(f), 135 Stat. 429, 953 (codified 16 U.S.C. 824s–1(f)) (emphasis added).

[395] *See Incentives for Advanced Cybersecurity Investment,* 180 FERC ¶ 61,189, at P 2 (2022) (citation omitted) (Cybersecurity Incentives NOPR); *id.* PP 24, 50–51; *see also id.* P 51 (''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.'') (emphasis added); *id.* P 51 n.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.'').

[396] *See, e.g., Am. Fed. Of Labor & Congress of Indus. Org.* v. *Donovan,* 757 F.2d 330, 339 (D.C. Cir. 1985) (''the modification cannot reasonably be seen as the 'logical outgrowth' of a proposal that gave no indication of any change at all in this respect.''); *Shell Oil Co.* v. *EPA,* 950 F.2d 741, 751 (D.C. Cir. 1991) (''Even if the mixture and derived-from rules had been widely anticipated, comments by members of the public would not in themselves constitute adequate notice. Under the standards of the APA, 'notice necessarily must come—if at all—from the Agency.'''') (citations omitted); *id.* (''Moreover, while a comment may evidence a recognition of a problem, it can tell us nothing of how, or even whether, the agency will choose to address it.'').

[397] *See* 5 U.S.C. 553.

[398] Final Rule, 183 FERC ¶ 61,033 at P 28.

[399] Public Law 117–58, section 40123(c)(2), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(c)(2)).

[400] *Id.,* section 40123(a), 135 Stat. 429, 951–52 (codified 16 U.S.C. 824s–1(a)).

[401] Cambridge Dictionary, *https://dictionary.cambridge.org/us/dictionary/english/enhance* (defining ''enhance'').

[402] Public Law 117–58, section 40123(c), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(c)).

the IIJA.[403] Congress knows how to say ''materially improve,'' and in fact, did so elsewhere in the IIJA,[404] but did not do so to limit the cybersecurity investments eligible for an incentive.

11. To make matters worse, the majority provides no meaningful objective criteria for satisfying its materiality requirement. While the Final Rule lists specific sources that the Commission will ''consider'' in its determination,[405] even when parties demonstrate that an investment meets the requisite number of sources the Commission finds that it does not ''have a *high degree of confidence* that such item[ ] will likely materially improve cybersecurity.'' [406] What could be more arbitrary than a ''standard'' based upon how confident an agency feels?

12. *Third,* the majority eliminates the 200-basis point ROE Adder incentive because ''[cybersecurity] expenses . . . constitute a large portion of overall expenditures for many cybersecurity investments'' and ''the Cybersecurity Regulatory Asset Incentive alone provides the encouragement that Congress intended without unduly increasing costs on consumers.'' [407] I disagree. Like Chairman Phillips, then Commissioner, stated in his concurrence to the NOPR:

> I believe the 5-year proposed duration and the 200-basis point adder are adequate to properly incent utilities. Unlike expenses in the traditional transmission incentives context, 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.[408]

13. Moreover, Congress required the Commission to establish a rule to provide incentives to investments in ''*any* technology, operational capability, or service'' [409] not just ''many cybersecurity investments.'' [410]

14. *Finally,* Congress did not require the Commission to simply ''consider performance-based rates as an option among incentive ratemaking treatments'' [411] as the majority contends. The statutory text states that ''the Commission *shall establish, by rule, incentive-based, including performance-based, rate treatments.*'' [412] There is no ambiguity here that could allow for, or support, the majority's ''interpretation.''

15. The word ''consider[ ],'' while used elsewhere in FPA section 219A,[413] is absent from that provision. And the majority should not place too much weight on Order No. 679, which interpreted a provision in FPA section 219 similarly.[414] The Commission's interpretation in Order No. 679 was arguably not in accordance with law and was never upheld by a court on appeal. My colleagues cannot rewrite a Congressional mandate because they believe that the statute is ''difficult'' to implement.[415]

16. Nor is compliance with this provision as ''difficult'' as the majority claims. The Commission could comply simply by establishing a rule that entities can propose on a case-by-case basis a performance-based rate treatment that would measure and tie the rate treatment to the number and severity of cybersecurity incidents. No more is required on the Commission's part.

17. Congress has made it clear that the Commission must provide incentives to shore up the security of the bulk power system. President Biden has ''urge[d] our private sector partners to harden [their] cyber defenses immediately.'' [416] Former President Trump issued an Executive Order declaring that ''[i]t is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure.'' [417] Former President Obama warned that cybersecurity threats are ''the most serious economic and national security challenge[ ] we face as a nation'' and ''America's economic prosperity . . . will depend on cybersecurity.'' [418] Similarly, last fall in his concurrence to the Cybersecurity Incentives NOPR, Chairman Phillips, then Commissioner, stated, ''the nation's security and economic well-being depends on reliable and cyber-resilient energy infrastructure.'' [419] Instead of following Congress' instructions, and taking this reliability threat seriously, the majority passes up the opportunity to harden the cybersecurity defenses of the nation's critical energy infrastructure.

For these reasons, I respectfully dissent.

James P. Danly,
Commissioner.

[FR Doc. 2023–08929 Filed 5–2–23; 8:45 am]

BILLING CODE 6717–01–P

---

[403] Final Rule, 183 FERC ¶ 61,033 at P 42.

[404] *See* Public Law 117–58, section 22420(a), 135 Stat. 429, 749 (''The Administrator of the Federal Railroad Administration shall conduct a study of the potential installation and use in new passenger rail rolling stock of passenger rail vehicle occupant protection systems that could *materially improve* passenger safety.''). *C.f. Cent. Bank of Denver* v. *First Interstate Bank,* 511 U.S. 164, 176–77 (1994) (''Congress knew how to impose aiding and abetting liability when it chose to do so.'') (citation omitted).

[405] Final Rule, 183 FERC ¶ 61,033 at P 40 (''Considering these sources as part of a Commission determination of whether a particular cybersecurity investment would materially improve cybersecurity''); *id.* P 109 (''the Commission will consider evidence'').

[406] *Id.* P 90.

[407] *Id.* P 134 (''We decline to adopt an ROE incentive adder, as proposed in the NOPR.'').

[408] Cybersecurity Incentives NOPR, 180 FERC ¶ 61,189 (Phillips, Comm'r, concurring, at P 7) (citations omitted).

[409] Public Law 117–58, section 40123(a), 135 Stat. 429, 951 (codified 16 U.S.C. 824s–1(a)) (emphasis added).

[410] Final Rule, 183 FERC ¶ 61,033 at P 134.

[411] *Id.* P 159.

[412] Public Law 117–58, section 40123(c), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(c)) (emphasis added).

[413] *Id.,* section 40123(d), 135 Stat. 429, 952 (codified 16 U.S.C. 824s–1(d)) (*i.e.,* factors for consideration).

[414] *See* Final Rule, 183 FERC ¶ 61,033 at P 159 (citing *Promoting Transmission Investment through Pricing Reform,* Order No. 679, 116 FERC ¶ 61,057, at P 270 (2006)).

[415] *Id.* P 160.

[416] *Statement by President Biden on Our Nation's Cybersecurity,* The White House (Mar. 21, 2022), *https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity; see also* Cybersecurity Incentives NOPR, 180 FERC ¶ 61,189 (Phillips, Comm'r, concurring at P 8 n.17) (quoting *Statement by President Biden on Our Nation's Cybersecurity*).

[417] Exec. Order No. 13800, 82 FR 22391, section 2 (May 11, 2017).

[418] *Remarks by the President on Securing Our Nation's Cyber Infrastructure,* The White House (May 29, 2009), *https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure#:~:text=In%20short%2C%20America%27s%20economic%20prosperity%20in%20the%2021st,them%20for%20public%20transportation%20and%20air%20traffic%20control.*

[419] Cybersecurity Incentives NOPR, 180 FERC ¶ 61,189 (Phillips, Comm'r, concurring at P 1).