173 FERC ¶ 61,240
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 35

[Docket No. RM21-3-000]

Cybersecurity Incentives

(December 17, 2020)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Commission is proposing to revise its regulations to establish rules for incentive-based rate treatments for voluntary cybersecurity investments by a public utility for or in connection with the transmission or sale of electric energy subject to the jurisdiction of the Commission, and rates or practices affecting or pertaining to such rates for the purpose of ensuring the reliability of the Bulk-Power System.

DATES: Comments are due **[INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER].** Also, reply comments are due **[INSERT DATE 90 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER.**

ADDRESSES: Comments, identified by docket number, may be filed electronically at http://www.ferc.gov in acceptable native applications and print-to-PDF, but not in scanned or picture format. For those unable to file electronically, comments may be filed by mail or may be hand-delivered. Mailed comments should be addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE,

Washington, DC 20426. Hand-delivered comments should be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852.

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

FOR FURTHER INFORMATION CONTACT:

Jessica L. Cockrell (Technical Information)
Office of Energy Policy and Innovation
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8190
jessica.cockrell@ferc.gov

Craig W. Barrett (Technical Information)
Office of Energy Infrastructure Security
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8830
craig.barrett@ferc.gov

Andrés López Esquerra (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6128
andres.lopez@ferc.gov

Adam Batenhorst (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6150
adam.batenhorst@ferc.gov

SUPPLEMENTARY INFORMATION:

173 FERC ¶ 61,240
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Docket No. RM21-3-000

NOTICE OF PROPOSED RULEMAKING

(December 17, 2020)

TABLE OF CONTENTS

Paragraph Numbers

I. Introduction ..... 1.

II. Background ..... 5.
A. Critical Infrastructure Protection Reliability Standards ..... 5.
B. NIST Framework ..... 10.
C. Transmission Incentives Notice of Inquiry and Rulemaking ..... 12.
D. Cybersecurity Incentives Policy White Paper ..... 14.

III. Need for Reform ..... 17.

IV. Discussion ..... 20.
A. Cybersecurity Incentives Framework ..... 20.
B. Applicable Cybersecurity Investments ..... 21.
1. NERC CIP Incentives Approach ..... 22.
2. NIST Framework Approach ..... 32.
C. Incentives for Cybersecurity Investments ..... 38.
1. ROE Adder ..... 38.
2. Regulatory Asset Incentive ..... 40.
3. Other Types of Incentives ..... 47.
D. Application Process ..... 48.
1. NERC CIP Incentives Approach ..... 50.
2. NIST Framework Approach ..... 54.
3. ROE Adder ..... 57.
4. Regulatory Asset Incentive ..... 58.
E. Implementation ..... 59.
1. Incentive Duration ..... 59.
2. Informational Filing and Verification ..... 61.
3. Confidentiality Considerations ..... 74.

V. Information Collection Statement ..... 76.
VI. Environmental Analysis..... 92.
VII. Regulatory Flexibility Act ..... 93.
VIII. Comment Procedures ..... 97.
IX. Document Availability..... 100.

I. Introduction

1. In this Notice of Proposed Rulemaking (NOPR), the Federal Energy Regulatory Commission (Commission) proposes under sections 205 and 206 of the Federal Power Act (FPA)[1] to establish rules for incentive-based rate treatments for voluntary cybersecurity investments[2] by a public utility.[3] These rules would provide cybersecurity incentives to public utilities that make certain cybersecurity investments that go above and beyond the requirements of the CIP Reliability Standards,[4] and materially enhance the cybersecurity posture of the Bulk-Power System[5] by enhancing the applicants'

[1] 16 U.S.C. 824d, 824e.

[2] Voluntary cybersecurity investments refer to cybersecurity investments not required to meet mandatory North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Reliability Standards (CIP Reliability Standards).

[3] The proposed incentive-based treatments for cybersecurity investments would also be available to non-public utilities to the extent that they have Commission-jurisdictional rates.

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 73 FR 7367 (Feb. 7, 2008),122 FERC ¶ 61,040, at P 1, *order on reh'g and clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*¸ Order No. 706-B, 74 FR 12544 (Mar. 25, 2009), 126 FERC ¶ 61,229, *order denying clarification*, Order No. 706-C, 74 FR 30067 (June 24, 2009), 127 FERC ¶ 61,273 (2009).

[5] Bulk-Power System is defined by FPA section 215 as facilities and control

cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers.

2. First, we propose to allow public utilities making certain cybersecurity investments to request an increase in the rate of return on equity (ROE) applicable to those capital investments. Such cybersecurity investments would include investments following specific CIP Reliability Standards and/or standards and guidelines from the National Institute of Standards and Technology (NIST)[6] Framework.

3. Second, we propose to allow a public utility to seek deferred cost recovery for certain cybersecurity investments. We propose that only expenses for activities that go above and beyond actions required to comply with the CIP Reliability Standards be eligible for these incentives. Therefore, expenses incurred to comply with mandatory CIP Reliability Standards that a public utility incurs on a regular or ongoing basis, or that are incurred prior to the incentive request, would not be eligible for such regulatory asset treatment. We propose to allow deferred cost recovery for three categories of expenses:

---

systems necessary for operating an interconnected electric energy transmission network (or any portion thereof), and electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. 825o(a).

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

(1) expenses associated with third-party provision of hardware, software, and computing networking services; (2) expenses for training to implement new cybersecurity enhancements undertaken pursuant to this rule; and (3) other implementation expenses, such as risk assessments[7] by third parties or internal system reviews and initial responses to findings of such assessments. In all such cases, eligible costs would be limited to costs associated with implementing cybersecurity upgrades and would not include ongoing costs including system maintenance, surveillance, and other labor costs, either in the form of employee salaries or third-party service contracts. Furthermore, we propose that the deferred regulatory assets whose costs are typically expensed should be amortized over a five-year period.

4. Finally, under the proposed regulations, a public utility seeking one or more incentive based-rate treatments proposed in the NOPR must make a filing for Commission approval pursuant to FPA section 205 and receive such approval prior to implementing the proposed incentives in its Commission-jurisdictional rates.

[7] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, at 26 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

II. Background

A. Critical Infrastructure Protection Reliability Standards

5. On August 8, 2005, Congress enacted the Energy Policy Act of 2005.[8] The Energy Policy Act of 2005 added a new section 215 to the FPA,[9] which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards,[10] including requirements for cybersecurity protection, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the Electric Reliability Organization subject to Commission oversight, or the Commission can independently enforce Reliability Standards.

6. On February 3, 2006, the Commission issued Order No. 672,[11] implementing FPA section 215. The Commission subsequently certified NERC as the Electric Reliability

[8] Energy Policy Act of 2005, Pub. L. No. 109-58, secs. 1261 *et seq.*, 119 Stat. 594 (2005).

[9] 16 U.S.C. 824o.

[10] FPA section 215 defines Reliability Standard as a requirement, approved by the Commission, to provide for reliable operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the Bulk-Power System. However, the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity. *Id.* at 824o(a)(3).

[11] *Rules Concerning Certification of the Elec. Reliability Org.; and Procedures for the Establishment, Approval, and Enf't of Elec. Reliability Standards*, Order No. 672, 71 FR 8661 (Feb. 17, 2006), 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 71 FR 19814 (Apr. 28, 2006), 114 FERC ¶ 61,328 (2006).

Organization. The Reliability Standards developed by NERC become mandatory and enforceable after Commission approval and apply to users, owners, and operators of the Bulk-Power System, as set forth in each Reliability Standard.[12] The CIP Reliability Standards require entities to comply with specific requirements to safeguard critical cyber assets. These standards are results-based and do not specify a technology or method to achieve compliance, instead leaving it up to the entity to decide how best to comply.

7. On January 18, 2008, the Commission issued Order No. 706,[13] approving the initial eight CIP Reliability Standards, CIP version 1 Standards, submitted by NERC. Subsequently, the Commission has approved multiple versions of the CIP Reliability Standards submitted by NERC, partly to address the evolving nature of cyber-related threats to the Bulk-Power System. On November 22, 2013, the Commission issued Order No. 791,[14] approving CIP version 5 Standards, the last major revision to the CIP Reliability Standards. The CIP version 5 Standards implement a tiered approach to

[12] NERC uses the term "registered entity" to identify users, owners, and operators of the Bulk-Power System responsible for performing specified reliability functions with respect to NERC Reliability Standards. *See*, *e.g.*, *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 FR 24594 (Apr. 25, 2012), 139 FERC ¶ 61,058, at P 46, *order denying clarification and reh'g*, 140 FERC ¶ 61,109 (2012). Within the NERC Reliability Standards are various subsets of entities responsible for performing various specified reliability functions. We collectively refer to these as "entities."

[13] Order No. 706, 122 FERC ¶ 61,040 at P 1.

[14] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 FR 72755 (Dec. 13, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

categorize assets, identifying them as high, medium, or low risk to the operation of the Bulk Electric System (BES)[15] if compromised. High impact systems include large control centers. Medium impact systems include smaller control centers, ultra-high voltage transmission, and large substations and generating facilities. The remainder of the BES Cyber Systems[16] are categorized as low impact systems. Most requirements in

[15] In general, NERC defines BES to include all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. *See* NERC, *Bulk Electric System Definition Reference Document*, Version 3, at page iii (August 2018). In Order No. 693, the Commission found that NERC's definition of BES is narrower than the statutory definition of Bulk-Power System. The Commission decided to rely on the NERC definition of BES to provide certainty regarding the applicability of Reliability Standards to specific entities. *See Mandatory Reliability Standards for the Bulk-Power System,* Order No. 693, 72 FR 16415 (Apr. 4, 2007), 118 FERC ¶ 61,218, at PP 75, 79, 491, *order on reh'g*, Order No. 693-A, 72 FR 49717 (July 25, 2007), 120 FERC ¶ 61,053 (2007).

[16] NERC defines BES Cyber System as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC, Glossary of Terms Used in NERC Reliability Standards, at 5 (2020), https://www.nerc.com/files/glossary_of_terms.pdf (NERC Glossary of Terms). NERC defines BES Cyber Asset as

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Id. at 4.

the CIP Reliability Standards apply to high and medium impact systems; however, a technical controls requirement in CIP-003, described below, applies only to low impact systems. Since 2013, the Commission has approved new and modified CIP Reliability Standards that address specific issues such as supply chain risk management, cyber incident reporting, communications between control centers, and the physical security of critical transmission facilities.[17]

8. The CIP Reliability Standards currently consist of 12 standards specifying a set of requirements that entities must follow to ensure the cyber and physical security of the Bulk-Power System. There are 10 currently effective cybersecurity standards and one cybersecurity standard that has been approved by the Commission and will become enforceable on July 1, 2022. There is also one physical security standard, which is not the subject of this NOPR:[18]

- CIP-002-5.1a Bulk Electric System Cyber System Categorization: requires entities to identify and categorize BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that

[17] *See, e.g.,* Order No. 791, 78 FR 72755; *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 81 FR 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016); *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032 (2018).

[18] CIP-014-2—Physical Security: requires entities to identify and protect transmission stations and transmission substations, and their associated primary control centers, that, if rendered inoperable or damaged as a result of a physical attack, could result in instability, uncontrolled separation, or cascading within an interconnection.

loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

- CIP-003-8 Security Management Controls: requires entities to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- CIP-004-6 Personnel and Training: requires entities to minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
- CIP-005-6 Electronic Security Perimeter(s): requires entities to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- CIP-006-6 Physical Security of Bulk Electric System Cyber Systems: requires entities to manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- CIP-007-6 System Security Management: requires entities to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- CIP-008-5 Incident Reporting and Response Planning:[19] requires entities to mitigate the risk to the reliable operation of the BES as the result of a cybersecurity incident by specifying incident response requirements.
- CIP-009-6 Recovery Plans for Bulk Electric System Cyber Systems: requires entities to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
- CIP-010-3 Configuration Change Management and Vulnerability Assessments: requires entities to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.
- CIP-011-2 Information Protection: requires entities to prevent unauthorized access to BES Cyber System Information by specifying

[19] An update to CIP-008-6 Reliability Standard will become enforceable on January 1, 2021.

information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

- CIP-012-1 Communications between Control Centers:[20] requires entities to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
- CIP-013-1 Supply Chain Risk Management: requires entities to mitigate cybersecurity risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.

9. The CIP Reliability Standards, viewed as a whole, implement a defense-in-depth approach to protecting the security of BES Cyber Systems at all impact levels.[21] The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.[22]

B. NIST Framework

10. The Cybersecurity Enhancement Act of 2014 (Cybersecurity Act)[23] updated the role of the NIST to include identifying and developing cybersecurity risk frameworks for

[20] CIP-012-1: Communications between Control Centers will be subject to enforcement by July 1, 2022.

[21] Order No. 822, 154 FERC ¶ 61,037 at 32.

[22] Order No. 706, 122 FERC ¶ 61,040 at 72.

[23] 15 U.S.C. 272(e)(1)(A)(i).

voluntary use by critical infrastructure owners and operators. Under the Cybersecurity Act, NIST must identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.[24]

11. As noted above, NIST implements the Cybersecurity Act through its NIST Framework,[25] which provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are currently working effectively in industry.[26] The Cybersecurity Framework incorporates voluntary consensus standards and industry best practices to the fullest extent possible.[27] The NIST Framework consists of three parts: Framework Core; Implementation Tiers; and Framework Profiles.[28] The Framework Core is a set of cybersecurity activities,

---

[24] 15 U.S.C. 272 (e)(1)(A)(iii). Security Controls is defined as follows: the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. NIST, *Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/security_controls.

[25] Version 1.0 of the NIST Framework was released in 2014, and subsequently replaced with version 1.1 in 2018.

[26] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, at v (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[27] *See* Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737 (Feb. 19, 2013).

[28] NIST Framework at v.

outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Framework Core provide detailed guidance for developing individual Framework Profiles.[29] Through use of Framework Profiles, the NIST Framework is designed to help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for an organization to view and understand the characteristics of its approach to managing cybersecurity risk, which is designed to help in prioritizing and achieving cybersecurity objectives.[30] The Framework Core consists of five concurrent and continuous Functions – Identify, Protect, Detect, Respond, and Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.[31]

C. Transmission Incentives Notice of Inquiry and Rulemaking

12. On March 21, 2019, the Commission issued a Notice of Inquiry seeking comment on the scope and implementation of its electric transmission incentives policy[32] to ensure

[29] *Id.*

[30] *Id.*

[31] *Id.* at 3.

[32] *Inquiry Regarding the Commission's Electric Transmission Incentives Policy*, 166 FERC ¶ 61,208 (2019) (2019 Notice of Inquiry).

that the policy continues to satisfy its obligations under FPA section 219.[33] The Notice of Inquiry included numerous questions regarding the Commission's approach to, and the objectives of, its transmission incentives policy; the mechanics and implementation of a transmission incentives policy; and metrics for evaluating the effectiveness of transmission incentives. As related to this proceeding, the Commission requested comment on whether it should incent physical and cybersecurity enhancements at transmission facilities and, if so, what types of security investments should qualify for transmission incentives.[34]

13. On March 20, 2020, the Commission issued a Notice of Proposed Rulemaking on several topics considered in the 2019 Notice of Inquiry.[35] In the Transmission Incentives NOPR, the Commission acknowledged that, although reliability is clearly delineated as a benefit to be promoted by transmission incentives, there are differing mandates for promoting reliability under FPA sections 215 and 219. Further, the Commission stated that cybersecurity is an important part of reliability and indicated that it would address cybersecurity incentives independently in a separate, future proceeding.[36]

---

[33] 16 U.S.C. 824s.

[34] 2019 Notice of Inquiry, 166 FERC ¶ 61,208 at P 27.

[35] *Electric Transmission Incentives Policy Under Section 219 of the Federal Power Act*, 85 FR 18784 (Apr. 2, 2020), 170 FERC ¶ 61,204, *errata notice*, 171 FERC ¶ 61,072 (2020) (Transmission Incentives NOPR).

[36] 2019 Notice of Inquiry, 166 FERC ¶ 61,208 at P 5.

D. Cybersecurity Incentives Policy White Paper

14. On June 18, 2020, Commission staff issued a white paper to explore a new framework for providing transmission incentives to public utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the CIP Reliability Standards.[37] In the White Paper, Commission staff discussed augmenting the current CIP Reliability Standards under FPA section 215 with an incentive-based framework under FPA section 219 that encourages public utilities to undertake cybersecurity investments on a voluntary basis. Commission staff reasoned that this framework would incent a public utility to adopt best practices to protect its own transmission system as well as improve the security of the BES. Further, Commission staff stated that the framework could allow the electric industry to be more agile in monitoring and responding to new and evolving cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions. Commission staff reasoned that an incentive-based framework would allow a public utility to tailor its request for incentives to the potential challenges it faces and take responsive action. Commission staff explained that, in the future, these voluntary actions taken by public utilities, if proven beneficial, could be the basis of future CIP Reliability Standards that would be mandatory.[38]

---

[37] *Cybersecurity Incentives Policy White Paper*, Notice of White Paper, Docket No. AD20-19-000 (issued June 18, 2020) (White Paper).

[38] *Id*. at 12-13.

15. Commission staff stated that providing transmission incentives for cybersecurity investments would require a new framework for the Commission to evaluate requests from public utilities for transmission incentives. Commission staff opined that a first necessary step would be to establish approaches that examine the effectiveness of cybersecurity investments in enabling the public utility to achieve a level of protection that exceeds the CIP Reliability Standards and also enhances the security of its transmission system. Commission staff stated that a public utility would then be able to identify the cybersecurity investments for which it seeks transmission incentives with the Commission evaluating such transmission incentive requests.

16. In the White Paper, Commission staff provided two potential approaches for identifying cybersecurity investments eligible for transmission incentives. The first approach was based on a public utility voluntarily applying certain CIP Reliability Standard requirements to transmission facilities that are not subject to those requirements, e.g., applying all requirements applicable to medium or high impact systems to low impact systems. The second approach was based on a public utility voluntarily implementing portions of the NIST Framework. Commission staff suggested that the two approaches could be used independently or in combination.[39]

[39] Commission staff noted that, under this potential approach, although a public utility could request a combination of incentives for its facility containing multiple assets, each individual asset would be eligible for only one cybersecurity incentive at a time.

III. Need for Reform

17. We recognize that the energy sector faces numerous and complex cybersecurity challenges. These growing threats come at a time of both great change in the operation of the transmission system and an increase in the number and nature of attack methods.[40] Encouraging utilities to address cybersecurity of the Bulk-Power System is uniquely important given the degree to which components of the Bulk-Power System are digitally interconnected with one another and the ever-expanding risks posed by adversaries create challenges for those tasked with defending those interconnections from cyber exploitation. In addition, a cybersecurity breach could have exponential effects on the Bulk-Power System. As the operating environment continues to change, there is the potential for increased vulnerabilities and amplification of cybersecurity threats to the Bulk-Power System. For example, as the Commission has previously explained, the global supply chain affords significant benefits to customers, including low cost, interoperability, rapid innovation, and a variety of product features.[41] Despite these benefits, the global supply chain creates opportunities for adversaries to directly or indirectly affect the management or operation of companies with potential risks to end users that could introduce new unintended threats to the system and necessitate rapid

[40] *See, e.g.*, Eversource Energy Serv. Co., Comments, Docket No. PL19-3-000, at 29-30 (filed June 26, 2019) (noting that market operations are becoming increasingly more complex at the same time that there is an increasing cybersecurity threat to the operation and control of the transmission system).

[41] *See, e.g. Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 FR 43354, 152 FERC ¶ 61,054, at PP 61-62 (2015).

mitigating actions.[42] Further, the COVID-19 national emergency[43] prompted many organizations to revise their operations to support an increased number of remote workers. The rapid expansion of teleworking capabilities revealed potential vulnerabilities, and some identified cybersecurity events specifically targeting remote access network equipment.[44] It is important that public utilities make cybersecurity investments to quickly and effectively address these cybersecurity challenges as well as other emerging threats. Therefore, the Commission has concluded that, given the unique importance of protecting the cybersecurity of the Bulk-Power System, it is appropriate to provide incentives for public utility cybersecurity investment as proposed in this NOPR.

18. Section 215 of the FPA and the CIP Reliability Standards promulgated under that statute have served as the Commission's primary tools for mandating changes to cybersecurity practices within the electric sector. As required by FPA section 215, the Commission's mandatory CIP Reliability Standards provide for the reliable operation of the Bulk-Power System.[45] Although the CIP Reliability Standards offer protection of the

---

[42] *Supply Chain Risk Management Reliability Standards,* Order No. 850, 165 FERC ¶ 61,020, at P 2 (2018).

[43] The Secretary of Health and Human Services declared a public health emergency on January 31, 2020, under section 319 of the Public Health Service Act (42 U.S.C. 247d), in response to COVID-19.

[44] Cybersecurity and Infrastructure Security Agency, National Cyber Awareness System Alerts, COVID-19 Exploited by Malicious Cyber Actors (Alert AA20-099A) (Apr. 8, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20099a#:~:text=Both%20CISA%20and%20NCSC%20are,threat%20to%20individuals%20and%20organizations.

[45] FPA section 215(a)(3) provides that the term reliability standard means a

BES[46] and improve the baseline cybersecurity posture of entities,[47] they have certain limitations. For example, it can take many months for a new Reliability Standard to be developed and, once approved, it may be several more months or years before a Reliability Standard is fully implemented and enforceable.[48] Further, the Bulk-Power System relies on the interdependence of connected networks and equipment; because the CIP Reliability Standards apply to BES facilities, which are generally 100 kV or higher as identified in CIP-002, not all cybersecurity systems are covered by these standards. Thus, while there are limits to how quickly CIP Reliability Standards can become mandatory and enforceable as well as limits to what the CIP Reliability Standards can cover, the cybersecurity threats public utilities face evolve and arise on their own timeframe. For these reasons, we believe that an effective strategy against emerging cybersecurity threats includes not only requiring public utilities to comply with the mandatory CIP Reliability Standards but also encouraging public utilities to make cybersecurity investments in addition to those required by the CIP Reliability Standards. We propose to do this by providing incentives to public utilities that voluntarily make

---

requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system.

[46] Order No. 791, 145 FERC ¶ 61,160 at PP 2, 41.

[47] Order No. 822, 154 FERC ¶ 61,037 at 2.

[48] *See, e.g.,* Am. Elec. Power, Inc., Comments, Docket No. PL19-3-000, at 13-14 (filed June 26, 2019) (noting that there is a potential gap between the dynamic threats faced by the energy industry and the CIP Reliability Standards development and compliance process, which sets the rules for minimum compliance).

certain cybersecurity investments above and beyond those investments required by the CIP Reliability Standards. The Commission proposes taking a two-prong approach to cybersecurity, which includes both mandatory CIP Reliability Standards and a cybersecurity incentives framework. This approach would encourage public utilities to increase the protection of their systems against cybersecurity threats. Currently, public utilities may not have the appropriate economic incentives to invest in cybersecurity measures that go above and beyond the mandatory CIP Reliability Standards. The cybersecurity incentives outlined in this NOPR strive to incent public utilities to use known, effective, and dynamic solutions to cybersecurity threats for the benefit of ratepayers.

19. Given that cybersecurity investments can be made to more than a public utility's transmission system, we find that basing our incentives framework under this proposal on our transmission incentives authority under FPA section 219, as considered in the White Paper, may unnecessarily limit the application of an effective cybersecurity incentives framework and, thereby, limit possible cybersecurity investment. Creating an incentive-based approach under FPA sections 205 and 206 that encourages public utilities to undertake cybersecurity investments on a voluntary basis that are above and beyond the requirements of the mandatory CIP Reliability Standards better ensures secure service for ratepayers. This approach would incent a public utility to adopt cybersecurity practices that would not only better protect its own systems but also improve the security of the Bulk-Power System. For example, the expansion of network monitoring provides the potential integration of all aspects of Bulk-Power System security to include physical

access control, equipment status indicators, and system performance monitoring. This provides for improved incident response time, pre-emptive planning, and system optimization. Further, relying on FPA sections 205 and 206 would allow public utilities to be more agile in monitoring and responding to new and unanticipated cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions. An incentive-based approach allows a public utility to tailor its request for incentives to the potential challenges and responsive actions that it faces. Finally, while we recognize that granting incentives to a public utility under this proposal will have an impact on the public utility's rates, we believe that such impact, over time, will be outweighed by the public utility having a more secure grid and services for the benefit of ratepayers.

IV. Discussion

A. Cybersecurity Incentives Framework

20. Pursuant to FPA sections 205 and 206,[49] we propose to add § 35.48 to the Commission's regulations to establish rules to provide incentive-based rate treatments for voluntary cybersecurity investments made by a public utility for or in connection with the transmission or sale of electric energy subject to the jurisdiction of the Commission. FPA sections 205 and 206 give the Commission authority over the rates of a public utility for or in connection with the transmission or sale of electric energy subject to the

[49] 16 U.S.C. 824d(a).

Commission's jurisdiction.[50] The Commission's FPA section 205 and 206 authority is broader than the Commission's authority under FPA section 219. FPA section 219 requires the Commission to issue a rule that provides incentive rate treatment for the transmission of electric energy in interstate commerce by public utilities for the purpose of benefitting consumers by ensuring reliability and reducing the cost of delivered power by reducing transmission congestion.[51] However, in this NOPR the Commission is proposing to provide incentives for a different purpose under a different section of the FPA: to provide incentives for cybersecurity investment not only in transmission facilities but also for cybersecurity investment in information technology and operational technology[52] networks that a public utility uses to provide other jurisdictional services. Reliance on FPA sections 205 and 206, therefore, allows for a more comprehensive way

[50] 16 U.S.C. 824d(a) (FPA section 205(a) provides that all rates and charges made, demanded, or received by any public utility for or in connection with the transmission or sale of electric energy subject to the jurisdiction of the Commission, and all rules and regulations affecting or pertaining to such rates or charges shall be just and reasonable); *see also FERC v. Elec. Power Supply Ass'n,* 136 S. Ct. 760, 774 (2016) (stating the Commission's FPA section 205 and 206 jurisdiction extends to practices that directly affect Commission-jurisdictional rates and that are not otherwise expressly excluded from the Commission's jurisdiction).

[51] 16 U.S.C. 824s(a).

[52] Operational technology is defined as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. NIST, Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/operational_technology.

to encourage cybersecurity investment than is available under FPA section 219. We believe that this comprehensive approach is warranted because cybersecurity threats to a public utility's system can come in a variety of forms, such as through a public utility's information technology and management systems, and not just through a public utility's systems that directly operate its transmission facilities. In addition, the means a public utility may need to use to protect against cybersecurity intrusions that may harm its jurisdictional system may not be limited to steps to protect the public utility's systems that run its transmission assets. Incentive ratemaking to encourage cybersecurity investments for not only those systems that are used to directly operate a public utility's transmission system but also other systems used for the provision of jurisdictional services is consistent with our general ratemaking authority under FPA sections 205 and 206 under which we may depart from cost-of-service ratemaking.[53] We believe that this action is appropriate to facilitate increased cybersecurity investment, and that the resulting rates will be just and reasonable.

B. Applicable Cybersecurity Investments

21. We propose to add § 35.48(b) to the Commission's regulations to authorize incentive-based rate treatments for a public utility that makes voluntary cybersecurity

[53] *Incentive Ratemaking for Interstate Natural Gas Pipelines, Oil Pipelines, & Elec. Utilities*, 61 FERC ¶ 61,168, at 61,594 (1992); *see also Farmers Union Cent. Exchange, Inc. v. FERC*, 734 F.2d 1486, 1503-04 (D.C. Cir. 1984) ("In some circumstances, the contrasting or changing characteristics of regulated industries may justify the agency's decision to take a new approach to the determination of 'just and reasonable' rates.").

investments in the Bulk-Power System, provided that the proposed incentive is just and reasonable and not unduly discriminatory or preferential.

1. NERC CIP Incentives Approach

22. We propose to add § 35.48(b)(1) to the Commission's regulations to provide that a public utility may receive incentive rate treatment for voluntarily applying identified CIP Reliability Standards to facilities that are not currently subject to those requirements (NERC CIP Incentives Approach). Using the existing CIP Reliability Standards as a framework for providing cybersecurity incentives allows the Commission to leverage an existing set of baseline cybersecurity requirements. Further, public utilities and the Commission are already familiar with the CIP Reliability Standards and encouraging public utilities to voluntarily apply known standards to additional facilities will establish a benchmark for determining eligibility for an incentive.

23. As discussed above, CIP-002 (Bulk Electric System Cyber System Categorization) implements a tiered approach to categorizing assets, requiring an entity to categorize its cyber assets as high, medium, or low risk to the reliable operation of the BES if compromised. These impact ratings determine which requirements in the CIP Reliability Standards CIP-003 though CIP-013 apply to BES Cyber Systems.

24. The CIP version 5 Standards became enforceable for high and medium impact BES Cyber Systems on July 1, 2016, and the CIP Reliability Standards applicable to low impact BES Cyber Systems became enforceable on April 1, 2020. In approving the CIP version 5 Standards, the Commission determined that "categorizing BES Cyber Systems based on their low, medium, or high impact on the reliable operation of the BES, with all

BES Cyber Systems being categorized as at least low impact, offers more comprehensive protection of the bulk electric system" and that "the new cybersecurity controls improve the security posture of responsible entities."[54]

25. We propose two ways for a public utility to demonstrate that it is eligible for a cybersecurity incentive through voluntary investment in applying the requirements of the CIP Reliability Standards to additional facilities. Public utilities that choose to request the proposed incentives under the NERC CIP Incentives Approach will receive a rebuttable presumption that the investments materially enhance the security posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards to merit an incentive for such cybersecurity investments.[55]

a. Med/High Incentive

26. We propose to add § 35.48(b)(1)(i) to the Commission's regulations to allow a public utility to receive incentive rate treatment for voluntarily applying the requirements for medium or high impact systems to low impact systems, and/or the requirements for high impact systems to medium impact systems (Med/High Incentive).

27. Under the Med/High Incentive, a public utility seeking a cybersecurity incentive for a facility that is classified as a low impact BES Cyber System would invest in ways to

---

[54] Order No. 791, 145 FERC ¶ 61,160 at P2.

[55] We do not propose that NERC will have any role in monitoring or reviewing the implementation of voluntary incentives or otherwise participating in this incentives program.

make that facility meet all the requirement and sub-requirement protections applicable to medium or high impact BES Cyber Systems. Also, under the Med/High incentive, a public utility seeking a cybersecurity incentive for a facility classified as a medium impact BES Cyber System would invest in ways to make that facility meet all the requirement and sub-requirement protections applicable to high impact BES Cyber Systems. The public utility could choose to apply the medium and/or high impact requirements to some or all of its low or medium impact BES Cyber Systems, and would receive incentives only for the investments it makes to apply the more stringent protections.

b. Hub-Spoke Incentive

28. We propose to add § 35.48(b)(1)(ii) to the Commission's regulations to allow a public utility to receive incentive rate treatment for voluntarily ensuring that all external routable connectivity[56] to and from the low impact system connect to a high or medium impact BES Cyber System (Hub-Spoke Incentive). Under the Hub-Spoke Incentive, a public utility is eligible for incentives if its investment applies CIP Reliability Standard security controls inherited from a high or medium impact BES Cyber System at locations containing low impact BES Cyber Systems by ensuring all external routable connectivity

[56] NERC defines external routable connectivity as "the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." NERC, Glossary of Terms Used in NERC reliability Standards (2020), https://www.nerc.com/files/glossary_of_terms.pdf.

to and from the low impact system connect to a high or medium impact BES Cyber System.

29. Under the Hub-Spoke Incentive, all the cyber communications to and from a low impact system location must connect to a medium or high impact BES Cyber System and the cyber communication security controls required for the medium or high impact BES Cyber System must be implemented on the low impact system.[57] Therefore, the cyber communication would be protected at a higher security level before being transmitted to or received by the low impact BES Cyber System. Thus, low impact BES Cyber Systems would inherit the higher security posture of either the medium or high impact controls.

c. Other Considerations

30. Nothing in this proposal modifies a public utility's obligation to comply with all the mandatory NERC Reliability Standard obligations for its low, medium, and high impact BES Cyber Systems. A public utility requesting incentive rate treatment for voluntarily applying the CIP Reliability Standards requirements, as discussed above, will not be subject to penalties from the Commission for failing to voluntarily follow the CIP Reliability Standards. However, if the Commission approves a public utility's request for cybersecurity incentives pursuant to either the Med/High or Hub-Spoke Incentive and the public utility subsequently ceases to implement the CIP Reliability Standards consistent with the order approving the application, we propose that the public utility would not be

[57] *See* proposed section 35.48(b)(1)(ii).

able to receive the incentive for the period during which it is not implementing the CIP Reliability Standards consistent with the order approving the application.

31. Additionally, since the NERC CIP Incentives Approach is based on a public utility making voluntary cybersecurity investments based on the CIP Reliability Standards as they exist at the time of the investment, we propose that the determination of the types of cybersecurity incentives that a public utility would be eligible for would reflect the currently enforceable version of the CIP Reliability Standards at the time the public utility submits a request for incentives. As discussed in section IV.E.1 (Incentive Duration), where NERC publicly announces that it is considering making certain cybersecurity activities or investments mandatory through issuing a standard authorization request,[58] a public utility would still be eligible to receive incentives until the requirements become mandatory and enforceable.

2. NIST Framework Approach

32. We propose to add § 35.48(b)(2) to the Commission's regulations to provide that a public utility may receive incentive rate treatment for implementing certain security controls included in the NIST Framework (NIST Framework Approach). The Commission would evaluate a public utility's application for cybersecurity investments that implement security controls in the NIST Framework to determine whether the

[58] A standard authorization request is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions, as well as document the benefit of retiring one or more approved Reliability Standards. NERC, Standard Authorization Request (SAR), https://www.nerc.com/pa/Stand/Pages/SARs.aspx.

cybersecurity investments go above and beyond the CIP Reliability Standards and are eligible for incentives. Through the NIST Framework Approach, public utilities have the flexibility of non-prescriptive implementation options to go above and beyond the CIP Reliability Standards.

33. Although the NIST Framework contains many types of security controls, we propose to limit eligibility for cybersecurity incentives to the types of controls that are most likely to provide a significant benefit to the cybersecurity of Commission-jurisdictional transmission facilities, not just the BES. In the White Paper, Commission staff identified five types of security controls included in the NIST Framework that may be considered for incentives under the NIST Framework approach: (1) automated and continuous monitoring; (2) access control; (3) data protection; (4) incident response; and (5) physical security of cyber systems. Commission staff also acknowledged that, given the continuous and rapid changes in cybersecurity risks, the Commission may need to periodically update the types of security controls eligible for incentives.[59] In proposing the NIST Framework Approach, we propose to initially only consider incentives that fall within the first type of security controls, automated and continuous monitoring. For example, continuous monitoring tools that utilize automated features for pulling information from a variety of sources or that allow for data consolidation into Security Information and Event Management tools would qualify as automated and continuous

[59] White Paper at 19.

monitoring security controls.[60] While this will limit the NIST Framework security controls eligible for incentives at this time, the Commission considers this to be an important next step in encouraging cybersecurity investments and may consider additional security control types in the future.

34. Under this proposal, one example of an investment that could warrant an incentive as automated and continuous monitoring would be for a public utility to install a dynamic asset management program to improve its ability to quickly detect and address new or previously unknown equipment on its network. Unknown and unattended equipment can present significant vulnerabilities and threats to both the information technology and operational technology networks. Implementing a process that automatically and continuously scans the current inventory of hardware and software across both the information technology and operational technology networks can identify, block, log and report any unauthorized access.

35. Another example of an automated and continuous monitoring investment eligible for an incentive is the implementation of a dynamic file analysis program or a "sandbox." One deployment of a sandbox is as an automated malware detection environment that continuously scans email attachments and weblinks in the corporate email system for malicious code. When malicious code is detected, a sandbox blocks delivery to the end user in real time and automatically issues an alert to the security team. Malicious code

[60] NIST, Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST Special Publication 800-137, at 13 (Sep. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

deployed in the sandbox will potentially be activated when placed there, but it will be isolated from the information technology and operational technology networks, thereby protecting the networks while alerting the public utility to the threat. The deployment of sandboxes enhances the ability of a public utility to detect and prevent the delivery of malicious code, disrupts social engineering attacks on users, and tests software for dangerous behavior. Further, the ability to perform post-incident forensic triage and analysis enables public utilities to establish the root causes of an event, identify related vulnerabilities, and mitigate associated risks in an expedited manner to optimize long-term operational capabilities.

36. As discussed below, public utilities seeking an incentive under this approach would need to show how a cybersecurity investment, for example, in physical components, software, licensing for cybersecurity enhancements as well as operational costs such as contracts with security providers, third-party incident responders, and third-party security operations centers, allows the public utility to meet NIST Framework security controls, as identified above, will go above and beyond the requirements of the CIP Reliability Standards, and materially enhance the current cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers. As the Commission evaluates incentive applications, we will remain cognizant of ongoing changes to the CIP Reliability Standards, the NIST Framework, and underlying referenced security controls.

37. As with the NERC CIP Incentives Approach, if a public utility ceases to maintain the cybersecurity posture associated with the Commission's order approving its NIST Framework Approach incentives application, the public utility would not be able to receive the incentive for the period during which it is not implementing the CIP Reliability Standards as described in the Commission's order approving its application.

C. Incentives for Cybersecurity Investments

1. ROE Adder

38. We propose to add § 35.48(c)(1) to the Commission's regulations to allow a public utility that makes eligible cybersecurity capital investments, as more fully described above, to request an ROE adder of 200 basis points (Cybersecurity ROE Incentives) for those eligible cybersecurity investments. This ROE incentive will encourage public utilities to proactively make additional investments in cybersecurity systems. We believe that such a 200-basis point adder is appropriate to provide a meaningful incentive to encourage public utilities to improve their systems' cybersecurity. For example, we note that given the relatively small size of such investments, compared to conventional transmission projects, the dollar amounts provided under the incentives should not have a burdensome effect on the public utility's rates. Yet, the benefit to the system, and ultimately to rate payers, by this additional investment will provide additional cybersecurity protections that could have a large impact on the public utility's system by allowing it to better detect and address cybersecurity threats to the Bulk-Power System. The total cybersecurity incentives requested would be capped at the zone of

reasonableness.[61] Additionally, we find that the same expenditures should not be eligible for both the Cybersecurity ROE Incentives and the Regulatory Asset Incentives discussed below. Given that regulatory asset treatment is available to costs that are normally treated as expenses, as discussed below, we believe that it is unnecessary to incent investment to also enable deferred costs that would otherwise be expensed to receive this 200 basis-point incentive. We propose that public utilities only be eligible to receive the Cybersecurity ROE Incentive as a cybersecurity incentive for capital investments.

39. Transmission-specific investments based on the NERC CIP Incentives Approach and the NIST Framework Approach may be eligible for the Cybersecurity ROE Incentive under this NOPR. In addition, we propose that enterprise-wide costs - which are not specific to transmission but a portion of which are recovered through transmission rates - may also be eligible for incentives if the applicant can demonstrate how the investment will materially enhance the security posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers. While cybersecurity systems that are not subject to the CIP Reliability Standards may be less critical to reliable operations, compromise of these systems may nevertheless allow access to more critical systems and therefore we believe that incentivizing the enhanced protection of these systems is important to the

[61] In the Transmission Incentives NOPR the Commission proposes that, under FPA section 219, the Commission may approve a rate that exceeds the zone of reasonableness to further the purposes of that statutory provision. In this NOPR, however, the Commission is acting under FPA sections 205 and 206.

reliability of the Bulk-Power-System.[62] Only the conventionally allocated portion of such investments that flows through to Commission jurisdictional cost-of-service rates will be eligible for this rate treatment. For instance, if a public utility seeks an incentive for cybersecurity investment that it made to its general plant facilities, both the underlying investments and associated incentives must be allocated based on conventions of the rates (e.g., the transmission share using a wages and salaries allocator for general plant in most transmission cost of service rates). With this limitation, we seek to ensure that the cybersecurity incentives policy adheres to the ratemaking principles of beneficiary pays and cost-causality by limiting a transmission customer's share of incentive costs to the share of such investments that serve (and is traditionally allocated to) transmission. We note that the Commission's rules and regulations in the Uniform System of Accounts[63] already require public utilities to maintain records supporting any entries to the regulatory asset account so that the utility can furnish full information as to the nature and amount of, and justification for, each regulatory asset recorded in the account. Therefore, pursuant to our existing regulations, public utilities must maintain

[62] For example, WANNACRY attacked specific servers that were vulnerable and once the attacker gained access to the server, the attacker moved to other internal systems to complete the attack. *See*, NCCIC, Fact Sheet, What is Wannacry/Wanacryptor?, https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf.

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

sufficient records to support the distinction of any expenses that are afforded incentivized treatment.[64]

2. Regulatory Asset Incentive

40. We propose to add § 35.48(c)(2) to the Commission's regulations to allow a public utility to seek deferred cost recovery pursuant to this NOPR. We believe that, in limited circumstances, it may be appropriate to allow a public utility to defer recovery of certain cybersecurity costs that are generally expensed as incurred, and treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base (Regulatory Asset Incentive). Such expenses must be associated with the NERC CIP Incentives Approach or the NIST Framework Approach investments that receive Commission approval for ROE incentives. Like the provision of ROE incentives, discussed above, we propose that only expenses for activities that go above and beyond the CIP Reliability Standards, as discussed above, be eligible for incentives. Under this proposal, expenses that are mandatory, that a public utility incurs on a regular or ongoing basis, or that are incurred prior to the incentive request, would not be eligible for such regulatory asset treatment.

41. More specifically, to implement proposed § 35.48(c)(2) of the Commission's regulations, we propose to allow deferred cost recovery for three categories of expenses: (1) expenses associated with third-party provision of hardware, software, and computing networking services; (2) expenses for training to implement new cybersecurity

[64] *Id.*

enhancements undertaken pursuant to this rule; and (3) other implementation expenses, such as system assessments by third parties or internal system reviews and initial responses to findings of such assessments. In all such cases, eligible costs are limited to costs associated with implementing cybersecurity upgrades and do not include ongoing costs including system maintenance, surveillance, and other labor costs, either in the form of employee salaries or third-party service contracts.

42. Regarding the first category, certain cost categories, such as software, that companies traditionally purchased and could capitalize, are now often procured as services with periodic payments to vendors that is updated as needed. Therefore, to encourage investment in cybersecurity, we believe that it would be appropriate to allow public utilities to defer and amortize eligible costs that are typically recorded as expense that are associated with third party provision of hardware, software, and computing and networking services. Pursuant to our existing regulations, public utilities must maintain sufficient records to support the distinction of any expenses that are afforded incentivized treatment.[65]

43. Regarding the second category, in response to the White Paper, many commenters stated that training is central to improving cybersecurity. We agree that such training is critical to successful implementation of cybersecurity enhancements. Therefore, we propose to allow public utilities to request the Regulatory Asset Incentive for training expenses associated with cybersecurity investments made pursuant to this rule. However,

[65] *Id.*

ongoing training expenses, which many organizations provide to employees regularly, would not be eligible because such training is an ongoing rather than implementation type of operating expense for the implementation we seek to incentivize. Pursuant to our existing regulations, public utilities must maintain sufficient records to support the distinction of any training expenses that are afforded incentivized treatment.[66]

44. Regarding the third category, we believe that there may be large one-time expenses associated with implementing cybersecurity upgrades. These may include unusually large internal system evaluations and assessments or analyses by third parties. These expenses may be large relative to the size of the capital investments associated with the cybersecurity upgrades and essential to their proper implementation. We propose that such expenses not include regularly scheduled activities that would occur irrespective of the cybersecurity upgrades. Pursuant to our existing regulations, public utilities must maintain sufficient records to support the distinction of any expenses that are afforded incentivized treatment.

45. Additionally, consistent with the proposal for the ROE incentive for eligible cybersecurity capital investments, only directly assigned transmission costs or the conventionally allocated (i.e., using the wages and salaries allocator) portion of enterprise-wide expenses would be eligible the Regulatory Asset Incentive. Applicants would be required under proposed § 35.48(b) to demonstrate that any enterprise-wide expenses for which they seek this treatment materially enhances the cybersecurity of the

[66] *Id.*

Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers.

46. Finally, we propose in § 35.48(d)(2) that deferred regulatory assets whose costs are typically expensed should be amortized over a five-year period. We believe that this duration will allow incentive recipients a reasonable amount of time to earn a return on expenditures for which no return is normally allowed. Moreover, the proposed amortization period generally corresponds to the short lifespan and depreciation rates of cybersecurity investments.

3. Other Types of Incentives

47. In this NOPR, we are proposing to grant ROE and deferred cost recovery incentives. Nonetheless, we recognize that other incentives, such as construction work in progress, may be warranted to encourage investment in cybersecurity if adequately supported. To maintain flexibility under this proposal for other types of incentives under these new regulations, we propose to add § 35.48(c)(3) to the Commission's regulations that provides the Commission additional flexibility to grant a public utility any other incentives, pursuant to the requirements of this section, that the Commission deems to be just and reasonable and not unduly discriminatory or preferential for investments undertaken pursuant to this rule.[67] We propose to consider applications for other

[67] We note that the Commission adopted similar flexibility and language to consider other proposals in section 35.35(d)(viii) of the Commission's rules and regulations in Order No. 679. *See* 18 CFR 35.35(d)(1)(viii); *Promoting Transmission Investment through Pricing Reform*, Order No. 679, 71 FR 43293 (Jul. 31, 2006), 116 FERC ¶ 61,057 (2006), *order on reh'g*, Order No. 679-A, 72 FR 1152 (Jan. 10, 2007),

cybersecurity incentives on a case-by-case basis to determine if they are just and reasonable and not unduly discriminatory or preferential under FPA section 205.

D. Application Process

48. Proposed § 35.48(e) of the Commission's regulations would require a public utility's request for one or more incentive based-rate treatments to be made in a filing pursuant to FPA section 205. As proposed, such a request must include a detailed explanation of how the public utility plans to implement one or both of the proposed incentive approaches and the requested rate treatment. We propose that applicants provide detail on the investments or expenses for which they seek incentives, as described in more detail below. An applicant would make a filing showing how its project(s) meet the eligibility requirements described below. In proposing what showing an applicant must make, we balance the need for sufficient information to determine if an applicant is eligible for the incentive against the risk of the applicant providing potentially sensitive information on cybersecurity vulnerabilities in its application. We discuss confidentiality concerns further in section IV.E.3 (Confidentiality Considerations).

49. Finally, under § 35.48(e) of the proposed regulations, a public utility seeking one or more incentive based-rate treatments proposed in the NOPR must make a filing for Commission approval pursuant to FPA section 205 and receive such approval prior to implementing the proposed incentives in its Commission-jurisdictional rates. In order to

---

117 FERC ¶ 61,345 (2006), *order on reh'g* 119 FERC ¶ 61,062 (2007).

effectuate the incentives in rates, public 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.[68]

1. NERC CIP Incentives Approach

50. To implement proposed § 35.48(b) of the Commission's regulations, for capital investments, we propose that an applicant describe the proposed investments as well as their anticipated cost, completion date and geographic location. An applicant would also describe how the proposed investment meets the description of the Med/High Incentive and/or the Hub-Spoke Incentive.

51. We propose that applicants describe the implementation and method of continuing adherence to the actions required to obtain and maintain the incentive, as described in § 35.48(e)(1) of the proposed regulations. The applicant would include in its application, at a minimum, an identification of the scope of assets for which the public utility is requesting the incentive, and the associated BES Cyber Systems that will be protected. Specifically, an applicant would include a list of BES assets for which the public utility is requesting the incentive, the geographical location of the BES assets, the function they support, the incentive method the public utility is requesting for each of the BES assets, the current impact ratings of the BES assets and the impact level(s) that the assets now

[68] Public 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.

meet as a result of the investment, and a list of BES Cyber Systems associated with each of the BES assets including details on their use.

52. Unlike conventional transmission investments, which entail completion of a physical transmission project, investments under the NERC CIP Incentives Approach seek to bring BES assets otherwise not required to be subject to certain cybersecurity requirements to a higher cybersecurity level, and that higher level must be maintained for it to continue to provide ratepayer benefits. Consequently, the Commission proposes that, if an investment that receives a Med/High Incentive or Hub-Spoke Incentive ceases to meet the requirements of that incentive, the public utility would be required to update its cost-of-service rates to reflect this change. In addition, the Commission or third parties may initiate FPA section 206 proceedings to revoke such incentives.

53. In Order No. 791, the Commission recognized that categorizing BES Cyber Systems based on their low, medium, or high impact on the reliable operation of the BES, with all BES Cyber Systems being categorized as at least low impact, offers more comprehensive protection of the BES than the prior CIP Reliability Standards.[69] The Commission also acknowledged that CIP version 5 Standards offer new cybersecurity controls that will improve the overall security posture of responsible entities.[70] Given the Commission's experience with the CIP Reliability Standards, we propose that an asset-by-asset showing of benefits is unnecessary because, though the benefits of upgrades may

[69] Order No. 791, 145 FERC ¶ 61,160 at P 41.

[70] *Id.*

vary by system, we believe that all upgrades based on the NERC CIP Incentives Approach materially enhance the cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers, and warrant incentives. Thus, we propose that a public utility seeking incentives under the NERC CIP Incentives Approach and that provides the information required under this application process receive a rebuttable presumption that the cybersecurity investments materially enhance the cybersecurity of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards to merit an incentive.

2. NIST Framework Approach

54. In contrast to applications for incentives based on the NERC CIP Incentives Approach, we propose that a public utility seeking incentives for cybersecurity investments under the NIST Framework Approach would not be entitled to a rebuttable presumption and instead must provide additional information showing that the proposed investment materially enhances the cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards. However, we request comments on what demonstration an applicant should be required to make to show that its NIST Framework Approach investments merit incentives under the FPA section 205 just and reasonable standard.

55. Depending on a public utility's existing attributes; namely the hardware, system configuration, and operating practices that contribute to its overall cybersecurity posture,

and the specific characteristics of the proposed cybersecurity investments, proposed cybersecurity investments may or may not materially enhance the cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards to warrant incentives. Under § 35.48(e)(2) of the Commission's regulations, we propose that an applicant must describe its current cybersecurity posture, desired cybersecurity posture, and the quantified risk factors being addressed through the proposed incentive actions. An application must include full and detailed explanations of how proposed cybersecurity investments will materially enhance the cybersecurity of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by CIP Reliability Standards, to the benefit of ratepayers. In assessing whether an application meets the standard for granting incentives under this NOPR, we propose that the Commission would review the stated expenditures and level of risk mitigated in comparison to the public utility's pre-incentivized network configuration. This judgement will be made on a case-by-case basis. The application would need to detail the specific components to be installed, network deployment, sensor configuration, and enterprise data incorporation as described in the four-step review process, discussed below.

56. Consistent with incentive requests under the NERC CIP Incentives Approach, an applicant seeking incentives under the NIST Framework Approach would be required to provide detail on the investments or expenses for which it seeks incentives. For capital investments, applicants would describe: (1) the required network components; (2) how

the sensors connect to the network; (3) how the sensors deployment recognizes the specific attributes of the network; (4) the costs of all investments; and (5) when the costs are expected to be incurred.

3. ROE Adder

57. Under § 35.48(e)(3) of the proposed regulations, applicants requesting an ROE adder of 200 basis points must include the anticipated cost of the capital investment and identify the Commission-jurisdictional rate schedules under which they will recover the ROE adder.

4. Regulatory Asset Incentive

58. For expenses that the applicant seeks to receive regulatory asset treatment associated with either ROE incentive-eligible projects based on either the NERC CIP Incentives Approach or the NIST Framework Approach, under § 35.48(e)(4) of the proposed regulations, the applicant must describe and estimate the nature of such expenses, their costs, and when they are expected to be incurred.[71] Applicants would be expected to provide a narrative explanation of how such expenses meet the description of the Med/High Incentive, the Hub-Spoke Incentive and/or the NIST Framework Approach. Applicants would then describe whether the expenses are: (1) expenses associated with third-party provision of hardware, software, and computing networking services; (2) expenses for training to implement new cybersecurity enhancements; or (3)

[71] We reiterate that applicants' ongoing costs of operating a more cybersecure system are not eligible for such incentive treatment under this NOPR.

other transition expenses, such as risk assessments[72] by third parties or internal system reviews, and initial responses to findings of such assessments. An applicant would also be required to describe the cost, location, and timing of all eligible capital investments and the cost and timing of all deferred expenses.

E. Implementation

1. Incentive Duration

59. We propose to add § 35.48(d) to the Commission's regulations to allow a public utility granted an incentive under this NOPR to receive that incentive for the lesser of: (1) the depreciation life of the underlying asset; (2) 10 years from when the cybersecurity improvements enter service; (3) when the investments or activities that serve as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission; or (4) when the public utility no longer meets the requirements for receiving the incentive.[73] We are seeking to incentivize cybersecurity assets that primarily include equipment or system modifications that typically have short depreciation lives. The cybersecurity incentives identified in this NOPR are intended to apply to technology and systems investments and not to more long-lived assets like physical structures. Thus, we believe that most public utilities granted cybersecurity

[72] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, at 26 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[73] FPA section 205 filings revising cost of service rates to implement incentives must contain language limiting incentive duration to the lesser of these three eventualities.

incentives under this NOPR should receive those incentives for the depreciation life of the asset. However, for investments with useful lives exceeding 10 years, we propose that the incentive end at the conclusion of 10 years from when the cybersecurity incentives enter service. Although it is possible that specific components of cybersecurity investments may feature longer useful lives than 10 years, given the evolving nature of cybersecurity threats, we find that 10 years is a reasonable expectation of the principal benefits of the cybersecurity investments, which should correspond to the investment duration.

60. In addition, we propose that, where cybersecurity investments are mandatory, cybersecurity incentives are inappropriate and would only serve to increase ratepayer costs. However, where NERC publicly announces that it is considering making certain cybersecurity activities or investments mandatory, through issuing a standard authorization request, public utilities may receive incentives until the requirements become mandatory. For a public utility that requests regulatory asset treatment for costs normally recorded to expenses, if such expenditures become mandatory, we propose that the public utility must recover the unamortized portion of expenses through expenses in rates with no further earning of an incentive return on the regulatory asset.

2. Informational Filing and Verification

61. In order to ensure that a public utility receiving incentive rate treatment has implemented the requirements for the incentive and to ensure that it continues to adhere to these requirements, we propose to add § 35.48(f) to the Commission's regulations to

require public utilities to submit annual informational filings with the Commission.[74] We propose specific reporting requirements for each of the NERC CIP Incentives Approach and the NIST Framework Approach below.

62. The Transmission Incentives NOPR proposes additional reporting requirements for recipients of transmission incentives under FPA section 219.[75] Such additional reporting is likewise appropriate for cybersecurity upgrades receiving incentives. Accordingly, we propose to add § 35.48(f) to require that, within 120 days of the completion of cybersecurity upgrades for which an applicant is granted incentives, an incentives recipient must make an informational filing and subsequent informational filings annually thereafter. The annual informational filings must detail the specific investments that were made pursuant to the Commission's approval and the corresponding FERC account(s) used. In addition, the annual informational filings must describe what parts of its network were upgraded or expanded (i.e., which substations, control centers, automated and continuous monitoring equipment) in addition to the nature (i.e., describing hardware purchase) and actual cost of the various capital investments. For incentives where the Commission allows deferral of expenses as regulatory assets, annual informational filings should describe such expenses in sufficient detail to demonstrate that such expenses are specifically related to implementing the

[74] These reporting requirements also apply to non-public utilities that receive cybersecurity incentives through their Commission-jurisdictional rates.

[75] Transmission Incentives NOPR, 166 FERC ¶ 61,208 at P 115.

cybersecurity incentives described in this NOPR and not for ongoing costs including system maintenance, surveillance, and other labor costs, either in the form of employee salaries or third-party service contracts.

63. We preliminarily find that the proposed reporting requirements are necessary to provide the Commission with an understanding of the costs of various types of cybersecurity investments in order to more precisely target future incentives or other policies. However, based on the qualities of such investments, as well as the likely higher sensitivity of the information, we propose to require different reporting requirements under this proposal than those proposed under the Transmission Incentives NOPR.

64. Several aspects of cybersecurity necessitate reporting different information that the Commission has required for conventional transmission facilities receiving incentives pursuant to FPA section 219. First, cybersecurity investments are not observable. Unlike conventional transmission facilities, such as a new transmission line, it is not readily apparent if, and when, such investments are completed and serving customers. Therefore, it is important to confirm the completion of cybersecurity investments by establishing additional reporting requirements. Second, certain cybersecurity investments may require public utilities to undertake subsequent actions or make expenditures to maintain the status for which they receive incentives. Annual reports enable public utilities to demonstrate that they have undertaken such actions or expenditures.

65. Finally, we propose that both the initial and annual informational filings provide a summary of the costs incurred to achieve the higher level of security, including

supporting documentation that provides a narrative explanation of the nature of the expenses proposed for deferred cost recovery, and inclusion in rate base as a regulatory asset, including the specific accounts (under the Commission's Uniform System of Accounts) initially charged for the incurred expenses.

66. Also, the Commission may conduct periodic verification to assess cybersecurity investments and expenses for which it has approved incentives. The Commission could perform such verifications through multiple means (i.e., directing further informational filings, audits, etc.). The annual informational filings will inform the Commission on how and when the additional verification is warranted.

a. NERC CIP Incentives Approach

67. To demonstrate that a public utility has implemented the requirements for the Med/High incentive and to ensure that the recipient continues to adhere to these requirements, we propose that the informational filing would describe implementation of the enhanced security controls, as applicable, in all the topics covered by the CIP Reliability Standards. Below is a table of currently effective and Commission-approved CIP Reliability Standards and examples of supporting documentation a public utility may provide to demonstrate incentive adherence to each CIP Reliability Standard. For the first informational filing, we would expect the public utility to provide documents, as indicated below, plus any additional documentation needed to demonstrate voluntary application of identified CIP Reliability Standards to facilities that are not currently

subject to those requirements.[76] For each subsequent annual informational filing, the public utility would only need to provide an updated version of the supporting documentation showing any changes from the prior informational filing as well as information on any period of time during the reported year where the public utility ceased to voluntarily apply identified CIP Reliability Standards to facilities that are not currently subject to those requirements.

[76] The information requested is similar to the information FERC staff reviews during a NERC CIP Reliability Standards audit.

Supporting Documentation Demonstrating Incentive Adherence		
Topic	Standard	Documentation
BES Cyber System Categorization	CIP-002[77]	List of the categorization of BES Cyber Systems included in the incentive
Management Controls	CIP-003	Senior Management approval of revised cyber security policies; updates to delegation procedures
Personnel and Training	CIP-004	Cyber security training program and quarterly reinforcement; personnel risk assessment program; access management program, and timely access revocation processes
Electronic Security Perimeters	CIP-005	Establishment of ESPs and management of electronic access points; remote access management
Physical Security of BES Cyber Systems	CIP-006	Physical security plans; visitor control program; PACS maintenance and testing procedures
Systems Security Management	CIP-007	Ports and services management; security patch management; malicious code prevention methods; security event monitoring; system access controls
Incident Reporting and Response	CIP-008	Cyber security incident response plan, implementation, and testing procedures
Backup and Recovery Plans	CIP-009	System recovery plans, implementation, and testing procedures
Configuration Change Management	CIP-010	System baseline configurations; configuration monitoring; vulnerability assessment processes
Information Protection	CIP-011	Information protection procedures; cyber asset reuse and disposal methods
Communications between Control	CIP-012[78]	Plans mitigating the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being

Centers		transmitted between any applicable Control Centers; and evidence of the associated security protections implemented and used
Supply Chain Risk Management	CIP-013	Supply chain security risk management plan, implementation, and testing procedures

68. To demonstrate that a public utility has implemented the requirements for the Hub-Spoke incentive, we propose that the informational filing describe the reconfiguration and assets added to the communication paths to/from locations containing low impact BES Cyber Systems. For the first annual informational filing, we propose that the public utility provide documents demonstrating these changes. For any subsequent annual informational filing, the public utility would only need to provide an updated version of any supporting documentation if a change occurred for the previous informational filing, as well as information on any failure to maintain the communication paths, and any mitigating actions the public utility undertook to resolve the problem.

b. NIST Framework Approach

69. We propose that the reporting requirements to implement proposed § 35.48(f) of its regulations for the NIST Framework Approach differ from those under the NERC CIP Incentives Approach. The Commission would review the informational filings to determine if the proposed changes meet the requirements for incentives by focusing on

[77] CIP-002 actions are not eligible for the incentive since it is a mandatory requirement for all BES assets.

[78] CIP-012-1: Communications between Control Centers will be subject to enforcement on July 1, 2022.

four areas: acquisition and installation, system connectivity, security application, and relevance to entity monitoring/response actions. For each subsequent annual informational filing, the public utility would only need to provide an updated version of the supporting documentation showing any changes from the prior informational filing, as well as information on any period of time during the reported year where the public utility ceased to continuously implement specific requirements consistent with the Commission's order approving the application.

70. Step 1 of the review process addresses the acquisition and installation of required network components (i.e., high-fidelity sensors) that meet the proposed security enhancements subject to incentives. The Commission would require a public utility to confirm that funds have been expended on the necessary equipment through documentation such as purchase orders, receipts, licensing agreements, and installation documentation with specified time periods.

71. Step 2 of the review process addresses the attainment of necessary training and personnel for the implementation of the incentivized action. Training and additional personnel must be necessary and limited to the implementation of the cybersecurity equipment within the affected networks. The Commission would require a public utility to verify training and personnel actions through documentation such as third-party contractor agreements, training program curricula, and official job descriptions.

72. Step 3 of the review process addresses network and sensor node recognition optimization of system deployment, and strategic configuration. This step describes how the sensors are connected to a network and how they substantively improve the visibility

and security of the affected networks. The public utility could demonstrate this network and sensor node recognition through such items as configuration files, system logs, configuration settings, and a description of its location on the affected network.

73. Step 4 of the review process addresses the incorporation of sensor nodes in the enterprise level incident monitoring and response plan. This step verifies that the incentivized action is being incorporated into monitoring and response actions to impact overall network security. The utility would need to attest that the information would be included in operational activities such as incident response plans, playbooks, and Standard Operating Procedures.

3. Confidentiality Considerations

74. We recognize that the Commission's cybersecurity incentives policy must balance the need to maintain the confidentiality of cybersecurity systems and protocols with the need for transparency in rates when awarding incentive rates to public utilities for cybersecurity investments. The Commission balances these considerations through its confidential[79] and Critical Energy/Electric Infrastructure Information (CEII) filing

[79] Section 388.112 of the Commission's regulations specifies that any person submitting a document to the Commission may request privileged treatment for some or all of the information contained in a particular document that it claims is exempt from the mandatory public disclosure requirements of the Freedom of Information Act and that should be withheld from public disclosure. In particular, section 388.112(b)(2) sets forth procedures for filing and obtaining access to material that is filed as privileged in any proceeding to which a right to intervention exists and specifies that if a person files material as privileged in such proceeding, that person must include a proposed form of protective agreement with the filing, or identify a protective agreement that has already been filed in the proceeding that applies to the filed material. 18 CFR 388.112.

regulations.[80] These regulations recognize that intervenors in a Commission proceeding, such as a proceeding establishing incentive rates, may need access to information that the applicant believes should be withheld from disclosure to the general public, in order to participate effectively in the proceeding. Therefore, the Commission's regulations provide for any person who is a participant in a proceeding or has filed a motion to intervene or notice of intervention to make a written request to the filer for a copy of the complete, non-public version of the document.

75. Accordingly, we propose that, if a public utility applying for incentive rate treatment under this rule is concerned that the information contained in an application for incentives could lead to the disclosure of confidential information or CEII related to its cybersecurity systems, the public utility could request protection of its information pursuant to these procedures. The Commission's practice, however, is not to allow for the filing of an FPA section 205 rate application under seal. Under this proposal, to the extent an applicant seeks confidential treatment, we expect that the applicant's request for such treatment will be specific and limited. If an applicant requests portions of the application be protected, we expect that the public portion of an application should contain sufficient information for ratepayers to judge the rate impact and scope of the proposed incentives, including the general approach adopted. The Commission will

[80] Section 388.113 governs the procedures for submitting, designating, handling, sharing, and disseminating CEII submitted to or generated by the Commission. Section 388.113(d)(1)(iii) provides for the person filing material as CEII in a proceeding to which a right to intervention exists to include a proposed form of protective agreement. 18 CFR 388.113.

address such requests for protection on a case by case basis.[81] We request comments on the specific and limited types of information that would be appropriate for applicants to shield from public disclosure, and any other specific modifications or additions to the Commission's generally applicable filing regulations that may be appropriate for the incentives filings proposed in this NOPR.

V. Information Collection Statement

76. The information collection requirements contained in this NOPR are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[82] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[83] 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 rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

77. This NOPR will establish the Commission's regulations and policy with respect to the mechanics and implementation of the Commission's cybersecurity incentives policy

[81] An applicant or any other person may object to disclosure generally or to a particular requester, and in such cases the non-public document will not be provided to the requester until ordered by the Commission or a decisional authority. 18 CFR 388.112(b)(2)(iv), 388.113(g)(4).

[82] 44 U.S.C. 3507(d).

[83] 5 CFR 1320.11.

and will require an annual report from the recipients of cybersecurity incentives in order to demonstrate compliance with the Commission's cybersecurity incentives regulations and policy.

78. 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).

79. The Commission solicits comments on the Commission's need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

80. Please send comments concerning the collection of information and the associated burden estimates to: Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street, NW, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission]. Due to security concerns, comments should be sent electronically to the following e-mail address: oira_submission@omb.eop.gov. Comments submitted to OMB should refer to OMB Control Nos.

81. Please submit a copy of your comments on the information collections to the Commission via the eFiling link on the Commission's website at http://www.ferc.gov. If you are not able to file comments electronically, please send a copy of your comments to:

Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426. Comments on the information collection that are sent to FERC should refer to RM21-3-000.

82. Title: Report of Cybersecurity Incentives Investment Activity.

83. Action: Proposed revision of collections of information in accordance with RM21-XX-000.

84. OMB Control Nos.: 1902-0248 (FERC-725B)

85. Respondents for this Rulemaking: Public Utilities that seek incentive-based rate treatment for cybersecurity projects.

86. Frequency of Information Collection: Annually beginning with the calendar year the Commission grants incentive-based rate treatment.

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

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

89. The NERC Compliance Registry, as of October 02, 2020, identifies approximately 319 Transmission Owners in the U.S. that are subject to this proposed rulemaking.

90. The Commission estimates that the NOPR would affect the burden[84] and cost[85] as follows:

Proposed Changes in NOPR in Docket No. RM21-3-000					
A. Area of Modification	**B. Number of Respondents**	**C. Annual Estimated Number of Responses per Respondent**	**D. Annual Estimated Number of Responses (Column B X Column C)**	**E. Average Burden Hours & Cost per Response**	**F. Total Estimated Burden Hours & Total Estimated Cost (Column D x Column E)**
Report of Cybersecurity Incentives Investment Activity					
Additional filers of Report of Cybersecurity Incentives Investment Activity (Annually and Ongoing)	20	1	20	80 hours; $6,640	1,600 hours; $132,800
Critical Infrastructure Protection Reliability Standards for FERC-725B (unchanged)	223,875	1	223,875	9.13 hours $757.44	2,043,026 hours; $169,571,158

[84] "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.

[85] Commission staff estimates that respondents' hourly wages (including benefits) are comparable to those of FERC employees. Therefore, the hourly cost used in this analysis is $83.00 ($172,329 per year).

Total			**223,895**		**2,044,626 hours;** **$169,703,958**

91. For the purposes of estimating burden in this NOPR, in the table above, we conservatively estimate annual numbers of the different possible cybersecurity incentive requests as similar to the historical high experienced for incentives Orders issued under Section 219. For example, to date, the Commission has received approximately 110 incentive requests since Order No. 679 was issued in 2006, and has issued an average of 8 incentives Orders per year, with a single year high of 21 incentive Orders issued. This estimate is consistent with our expectation that the cybersecurity incentives are likely to attract significant interest from the industry. We seek comment on the estimates in the table above regarding the number of incentive requests.

VI. Environmental Analysis

92. 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.[86] We conclude that neither an Environmental Assessment nor an Environmental Impact Statement is required for this proposed rule under § 380.4(a)(15) of the Commission's regulations, which provides a categorical exemption for approval of actions under FPA sections 205 and 206 relating to the filing of schedules

[86] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (1987) (cross referenced at 41 FERC ¶ 61,284).

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, classification, and services.[87]

VII. Regulatory Flexibility Act

93. The Regulatory Flexibility Act of 1980[88] generally requires a description and analysis of proposed and final rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) sets the threshold for what constitutes a small business. Under SBA's size standards,[89] Transmission owners all fall under the category of Electric Bulk Power Transmission and Control (NAICS code 221121), with a size threshold of 500 employees (including the entity and its associates).[90]

94. We estimate that 319 transmission owners are reported in the NERC registry. Using the list of Transmission Owners from the NERC Registry (dated October 2, 2020), we estimate that approximately 6% of those entities may file for incentives.

95. We estimate additional annual costs associated with the NOPR (as shown in the table above) of:

[87] 18 CFR 380.4(a)(15).

[88] 5 U.S.C. 601-612.

[89] 13 CFR 121.201

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

- $6,640 per filer for 20 new filers.
- These costs are only incurred on a voluntary basis.

96. Therefore, the estimated additional annual cost per entity ranges from $0 to $132,800. According to SBA guidance, the determination of significance of impact "should be seen as relative to the size of the business, the size of the competitor's business, the number of filers received annually (20), and the impact this regulation has on larger competitors."[91] We do not consider the estimated cost to be a significant economic impact. As a result, we certify that the proposals in this NOPR will not have a significant economic impact on a substantial number of small entities.

VIII. Comment Procedures

97. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due **[INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER].** Also, reply comments are due **[INSERT DATE 90 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. Comments must refer to Docket No. RM20-3-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

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

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

99. Commenters that are not able to file comments electronically may mail or hand-deliver an original of their comments. Mailed comments should be addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, DC 20426. Hand-delivered comments should be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

IX. Document Availability

100. 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).

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

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

List of Subjects in 18 CFR Part 35

Electric power rates

Electric utilities

Reporting and recordkeeping requirements

By direction of the Commission. Chairman Danly and Commissioner Glick are concurring with a joint separate statement attached. Commissioner Clements is not participating.

(S E A L)

Kimberly D. Bose,
Secretary.

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

Part 35 – FILING OF RATE SCHEDULES AND TARIFFS

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.

Subpart K – CYBERSECURITY INVESTMENT PROVISIONS

1. The authority citation for subpart K 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. Section 35.48 is added to read:

§ 35.48 Cybersecurity investment

(a) *Purpose.* This section establishes rules for incentive-based rate treatments for voluntarily making cybersecurity investments by a public utility as described in this subpart.

(b) *Incentive-based rate treatments for cybersecurity investment*. The Commission will authorize incentive-based rate treatments for a public utility that makes cybersecurity investments under this subpart that materially enhance the cybersecurity posture of the Bulk-Power System by enhancing the applicants' cybersecurity posture substantially above levels required by Critical Infrastructure Protection Reliability Standards, provided that the proposed incentive is just and reasonable and not unduly

discriminatory or preferential. A public utility may request one or both of the following incentive approaches for those eligible cybersecurity investments:

(1) *Critical Infrastructure Protection Incentive Approach*. A public utility may receive incentive rate treatment for voluntarily applying Critical Infrastructure Protection Reliability Standards to bulk electric system facilities that are not currently subject to those requirements. A public utility will receive a rebuttable presumption that the investments made pursuant to this Critical Infrastructure Protection Incentive Approach materially enhance the cybersecurity posture of the Bulk-Power System to merit an incentive for such cybersecurity investments. A public utility may receive incentive rate treatment for the investments as follows:

(i) Increasing the Critical Infrastructure Protection Reliability Standard security controls for facilities identified as low or medium impact bulk electric system Cyber Systems by applying the requirements for medium or high impact systems to low impact systems, and/or the requirements for high impact systems to medium impact systems; or

(ii) Ensuring all external routable connectivity to and from the low impact system connect to a high or medium impact bulk electric system Cyber System and the cyber communication security controls required for the medium or high impact bulk electric system Cyber System must be implemented on the low impact system.

(2) *National Institute of Standards and Technology Framework Approach*. A public utility may receive incentive rate treatment for implementing certain security controls, identified from time to time through a Commission issuance, that are included in the National Institute of Standards and Technology Framework.

(c) *Types of incentive-based rate treatments for cybersecurity investment.* For purposes of paragraph (b), incentive-based rate treatment shall be for those eligible cybersecurity investments and means any of the following:

(1) An increase in rate of return on equity of 200 basis points;

(2) Deferred cost recovery; or

(3) Any other incentives approved by the Commission, pursuant to the requirements of this section that are deemed to be just and reasonable and not unduly discriminatory or preferential.

(d) *Incentive duration.*

(1) A return on equity incentive rate treatment approved pursuant to this section may last the earlier of:

(i) the depreciation life of the underlying asset;

(ii) 10 years from when the cybersecurity improvements enter service;

(iii) when the investments or activities that serve as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission;

(iv) or when the public utility no longer meets the requirements for receiving the incentive.

(2) A deferred regulatory asset whose costs are typically expensed should be amortized over a five-year period.

(e) *Incentive Applications.* For the purpose of paragraphs (b) and (c), a public utility's request for one or more incentive based-rate treatments, to be made in a filing

pursuant to section 205 of the Federal Power Act, must include a detailed explanation of the proposed rate treatment and include the following information:

(1) For applications under the Critical Infrastructure Protection Incentive Approach:

(i) The Bulk Electric System assets for which the public utility is requesting the incentive;

(ii) The geographical location of the Bulk Electric System assets;

(iii) The function the Bulk Electric System assets support;

(iv) The incentive method the public utility is requesting for each of the Bulk Electric System assets;

(v) The current and new impact ratings of the Bulk Electric System assets if they change because of the incentive; and

(vi) A list of the Bulk Electric System Cyber Systems associated with each of the Bulk Electric System assets including details on their use.

(2) For applications under the National Institute of Standards and Technology Framework Approach:

(i)_A description of the public utility's current cybersecurity posture;

(ii) A description of the public utility's desired cybersecurity posture;

(iii) A description of the quantified risk factors being addressed through the proposed incentive actions.

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

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

(ii) The identity of the Commission jurisdictional rate schedule(s) under which it will recover the increased return on equity.

(4) For applications requesting deferred cost recovery:

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

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

(B) Expenses for training to implement new cybersecurity enhancements; or

(C) Other transition expenses, such as risk assessments by third parties or internal system reviews, and initial responses to findings of such assessments.

(ii) Estimates of the cost of such expenses;

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

(iv) A narrative explanation of how the expenses meet the requested Critical Infrastructure Protection Incentive Approach or National Institute of Standards and Technology Framework Approach.

(f) *Reporting requirements*. A public utility that has received cybersecurity incentives under this section must, within 120 days of completion of upgrades for which it receives incentives, make an informational filing and must make subsequent informational filings annually thereafter detailing the specific investments that were made pursuant to the Commission's approval and the corresponding FERC account used. An incentive recipient must describe the parts of its network that it upgraded in addition to the nature and cost of the various capital investments. For incentives where the

Commission allows deferral of expenses, annual informational filings should describe such expenses in sufficient detail to demonstrate that such expenses are specifically related to the cybersecurity investment granted incentives and not for ongoing services including system maintenance, surveillance, and other labor costs.

(1) A public utility that receives incentive-based rate treatment under the Critical Infrastructure Protection Incentive Approach must also describe in its informational filings implementation of the enhanced security controls, as applicable, in all the topics covered by the Critical Infrastructure Protection Reliability Standards. For the first informational filing, the public utility must provide documentation to demonstrate voluntary application of identified Critical Infrastructure Protection Reliability Standards to facilities that are not currently subject to those requirements. For subsequent annual informational filings, the public utility must provide an updated version of the supporting documentation showing any changes from the prior informational filing as well as information on any period of time during the reported year where the public utility ceased to voluntarily apply identified Critical Infrastructure Protection Reliability Standards to facilities that are not currently subject to those requirements.

(2) A public utility that receives incentive-based rate treatments under the National Institute of Standards and Technology Framework Approach must also include information that demonstrates:

(i) The acquisition and installation of required network components, including confirmation that funds have been expended on the necessary equipment through

documentation such as purchase orders, receipts, licensing agreements, and installation documentation with specified time periods;

(ii) Attainment of necessary training and personnel, including documentation such as third-party contractor agreements, training program curricula, and official job descriptions;

(iii) Network and sensor node recognition optimization through such items as configuration files, system logs, configuration settings, and a description of its location on the affected network;

(iv) Incorporation of sensor nodes in the enterprise level incident monitoring and response plan including attesting that the information would be included in operational activities such as incident response plans, playbooks, and Standard Operating Procedures.

Document Accession #: 20201217-3129 Filed Date: 12/17/2020

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Docket No. RM21-3-000

(Issued December 17, 2020)

DANLY, Chairman, and GLICK, Commissioner, *concurring*:

1. Threats to the cybersecurity of the bulk power system are numerous and growing. Ensuring that the system is adequately protected against those threats is an issue of national importance and one that must remain a priority of this Commission. Accordingly, we support this notice of proposed rulemaking (NOPR) as a means for soliciting further comments on whether this particular incentives-based approach is a just and reasonable and not unduly discriminatory or preferential approach to improving public utilities' cybersecurity posture.

2. We write separately to highlight two general issues that we believe require additional attention. The first issue is whether the Commission can better address cybersecurity threats by directing NERC to expand its critical infrastructure protection (CIP) standards to require some or all of the investments contemplated in this NOPR. Although we appreciate the appeal of an incentives-based approach, the importance of cybersecurity demands us to at least consider whether we should mandate the best practices contemplated in this NOPR rather than simply trying to induce public utilities to adopt them.

3. The second issue goes to the heart of what the NOPR intends to achieve—whether public utilities are not adopting the contemplated measures because the existing financial incentives are insufficient. We encourage commenters to address whether—and, if so, why—additional measures, such as an elevated ROE or deferred cost recovery, are necessary to incentivize public utilities to adopt additional cybersecurity measures.

For these reasons, we respectfully concur.

_____ _____

James P. Danly
Chairman

Richard Glick
Commissioner

Document Accession #: 20201217-3129 **Filed Date: 12/17/2020**

Document Content(s)

RM21-3-000.DOCX.....1