

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

CYBERSECURITY INCENTIVES POLICY WHITE Docket No. AD20-19-000
PAPER

NOTICE OF WHITE PAPER

(June 18, 2020)

Take notice that Commission staff is publishing a White Paper discussing a potential new framework for providing transmission incentives to utilities for cybersecurity investments.

The White Paper is being placed in the record of this administrative docket, referenced above. The White Paper will also be available on the Commission's website at <http://www.ferc.gov>.

Comments on the White Paper should be filed within 60 days of the issuance of this Notice and reply comments should be filed within 75 days of the issuance of this Notice. The Commission encourages electronic submission of comments in lieu of paper using the "eFiling" link at <http://www.ferc.gov>. Persons unable to file electronically should submit an original of the comment to the Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426.

All filings in this docket are accessible on-line at <http://www.ferc.gov>, using the "eLibrary" link. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed

docket. For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Questions regarding this Notice should be directed to:

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

Kimberly D. Bose,
Secretary.



Cybersecurity Incentives Policy White Paper

A STAFF PAPER: FEDERAL ENERGY REGULATORY COMMISSION
DOCKET NO. AD20-19-000

JUNE 2020

The opinions and views expressed in this staff paper do not necessarily represent those of the Federal Energy Regulatory Commission, its Chairman, or individual Commissioners, and are not binding on the Commission.

I. Introduction

In March 2019, pursuant to section 219 of the Federal Power Act (FPA),¹ the Commission issued a Notice of Inquiry seeking comment on the scope and implementation of its electric transmission incentives policy.² In March 2020, the Commission issued a Notice of Proposed Rulemaking on several topics considered in the 2019 Notice of Inquiry.³ In the Transmission Incentives NOPR, the Commission acknowledged that, although reliability is clearly delineated as a benefit to be promoted by incentives, there are differing mandates for promoting reliability under FPA sections 215⁴ 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. This staff paper discusses a potential new framework for providing transmission incentives to utilities for cybersecurity investments.

As discussed further in section II (Background) of this staff paper, pursuant to FPA section 215, the Commission has approved a suite of mandatory Reliability Standards that applicable registered entities must meet to provide for an adequate level of reliability of the bulk power system.⁵ FPA section 219(b)(4)(A) directs the Commission to establish rules allowing recovery of all prudently incurred costs necessary to comply with mandatory Reliability Standards.⁶ In light of these mandatory Reliability Standards, and the opportunity for cost recovery pursuant to FPA section 219(b)(4)(A), additional transmission incentives are not necessary to maintain an adequate level of reliability.

¹ 16 U.S.C. § 824s (2018). FPA Section 219(a) directs the Commission to establish incentive-based rate treatments to benefit consumers by ensuring reliability, and FPA section 219(b)(1) directs the Commission to promote reliable and economically efficient transmission. *Id.* § 824s(a)-(b)(1).

² *Inquiry Regarding the Commission’s Electric Transmission Incentives Policy*, 166 FERC ¶ 61,208 (2019) (2019 Notice of Inquiry).

³ *Electric Transmission Incentives Policy Under Section 219 of the Federal Power Act*, 84 Fed. Reg. 18,784 (Apr. 2, 2020), 170 FERC ¶ 61,204, *errata notice*, 171 FERC ¶ 61,072 (2020) (Transmission Incentives NOPR).

⁴ 16 U.S.C. § 824o (2018).

⁵ *Id.* § 824o(a)(3).

⁶ *Id.* § 824s(b)(4)(A). Pursuant to section 219(d), “[a]ll rates approved under the rules adopted pursuant to this section . . . are subject to the requirements of sections 205 and 206 that all rates, charges, terms, and conditions be just and reasonable and not unduly discriminatory or preferential.” *Id.* § 824s(d).

However, transmission incentives to counter the evolving and increasing threats to the cybersecurity of the electric grid may be warranted. This staff paper explores a new framework for providing transmission incentives to utilities for cybersecurity investments that produce significant cybersecurity benefits for actions taken that exceed the requirements of the Critical Infrastructure Protection Reliability Standards (CIP Reliability Standards).⁷

This staff paper first provides a background discussion, including a description of the cybersecurity challenges on the Bulk Electric System (BES)⁸ and existing CIP Reliability Standards. Next, it discusses the importance of infrastructure security, including the Commission and staff's efforts to incentivize energy infrastructure security to date, and why there is a need to adopt a new approach to incentivize cybersecurity investments. The staff paper then discusses an incentives framework for cybersecurity investment, including a description of various incentives and potential approaches to identify cybersecurity investments eligible for incentives. The staff paper also outlines the application process for utilities seeking incentives for cybersecurity investments from the Commission. Finally, the staff paper requests comments from interested parties on the topics discussed here, questions posed and whether the Commission should consider alternate approaches, within 60 days of the issuance of this paper and reply comments within 75 days of the issuance of this paper.

II. Background

A. The Cybersecurity Challenge

Securing the reliability, including cybersecurity, of energy infrastructure is a vital element in the protection of U.S. national security interests.⁹ The Commission is charged

⁷ *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 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, 126 FERC ¶ 61,229, *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

⁸ In general, NERC recognizes the 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). The terms BES (defined by NERC and adopted by the Commission) and bulk power system (a term defined in the EPAct 2005) are both used throughout this document.

⁹ Exec. Order No. 13,920, *Securing the U.S. Bulk-Power System*, 85 Fed. Reg. 26,595, at 26,595 (May 1, 2020).

with overseeing the development and enforcement of cybersecurity standards for the nation's BES. The electric transmission grid has many components that are vulnerable to cyber-attacks, and a cyber-attack against high voltage transformers or other large equipment used to support transformer functions can have a large impact on the transmission system due to the cost and time to replace these components.¹⁰ The risk of a cyber-attack to a utility responsible for transmission depends on several variables, such as network configuration within and between facilities and means of communicating data. A simultaneous cyber-attack on multiple electric grid facilities can have the effect of instantaneously dropping large amounts of load or generation from the grid.¹¹ Further, the electric grid is interconnected to other critical infrastructure and, due to the significant interdependencies between systems, adverse impacts to one system can materially impact others.¹² For these reasons, preventing or minimizing adverse impacts to energy infrastructure systems is crucial for maintaining a reliable energy system.

B. CIP Reliability Standards

On August 8, 2005, the Energy Policy Act of 2005 was enacted into law.¹³ EPAct 2005 added a new section 215 to the FPA, which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards, 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.¹⁴

¹⁰ Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, at 10 (Aug. 2016), <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>.

¹¹ See U.S. Gov't Accountability Office, *Critical Infrastructure Protection – Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, at 50-52 (Aug. 2019), <https://www.gao.gov/assets/710/701079.pdf>.

¹² For example, a cybersecurity incident that causes power plant outages or other electric disruptions could affect telecommunications, water supply, hospital services, financial transactions, and other essential services.

¹³ Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005) (EPAct 2005).

¹⁴ 16 U.S.C. § 824o(a)(3) (2018).

On February 3, 2006, the Commission issued Order No. 672, implementing FPA section 215.¹⁵ The Commission subsequently certified the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization.¹⁶ 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.

On January 18, 2008, the Commission issued Order No. 706, approving the initial eight CIP Reliability Standards submitted to the Commission for approval by NERC – CIP version 1.¹⁷ The CIP Reliability Standards require certain users, owners, and operators of the bulk power system 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 utility to decide how best to comply with the standards.

The CIP Reliability Standards have been modified over time, in part to address the evolving nature of cyber-related threats to the bulk power system. Since 2008, NERC has modified the CIP Reliability Standards, submitting new and modified standards for Commission approval. A major revision to the CIP Reliability Standards occurred in 2013, when the Commission approved CIP version 5 in Order No. 791, effective July 2016.¹⁸ The CIP version 5 Reliability Standards implemented a tiered approach to categorize assets, identifying them as high, medium, or low risk to bulk power system reliability 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 cyber systems are categorized as low impact systems. Most requirements in CIP Reliability Standards apply to high and medium impact systems; however, a technical controls requirement in CIP-003 applies only to low impact systems.¹⁹

¹⁵ *Rules Concerning Certification of the Elec. Reliability Org.; and Procedures for the Establishment, Approval, and Enf't of Elec. Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

¹⁶ *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

¹⁷ Order No. 706, 122 FERC ¶ 61,040 at P 1.

¹⁸ *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

¹⁹ CIP-003 otherwise applies to BES Cyber Systems of all impact ratings.

Since 2013, the Commission has approved new and modified CIP Reliability Standards that address specific issues such as the supply chain, cyber incident reporting, and physical security of critical transmission facilities.

The CIP Reliability Standards now consist of 13 standards specifying a set of requirements that registered entities must follow to ensure the cyber and physical security²⁰ of the bulk power system. There are currently 10 active cybersecurity standards and two cybersecurity standards to be effective in the near future:²¹

- **CIP-002-5.1a: Bulk Electric System Cyber System²² Categorization:** requires entities to identify and categorize BES cyber elements and their associated cyber assets for the application of cybersecurity requirements using a tiered approach commensurate with the adverse impact of their loss, compromise, or misuse.
- **CIP-003-7: Security Management Controls:** requires entities to specify consistent and sustainable security management controls to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- **CIP-004-6: Personnel and Training:** requires the minimizing of 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.

²⁰ There is one CIP Reliability Standard concerning physical security, which is not a subject of this staff paper. 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.

²¹ CIP-012-1: Communications between Control Centers will be subject to enforcement by July 1, 2022. CIP-013-1: Supply Chain Risk Management will be subject to enforcement by October 2020. In addition, updates to three CIP Reliability Standards will become enforceable over the next two years: CIP-005-6 and CIP-010-3 (enforceable by October 2020), and CIP-008-6 (enforceable by January 2021).

²² NERC defines a BES Cyber System as one 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/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (NERC Glossary of Terms).

- **CIP-005-5: 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:** 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-010-2: 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 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:** 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 by implementing security controls for supply chain risk management of BES Cyber Systems.

The CIP Reliability Standards, viewed as a whole, constitute a defense-in-depth²³ approach to cybersecurity based on an assessment of risk. The CIP Reliability Standards are objective-based and allow responsible entities to choose compliance approaches best tailored to their systems.

III. Infrastructure Security

A. Commission and Staff Efforts to Support Infrastructure Security

In conjunction with mandatory Reliability Standards, the Commission has used its authority to provide incentives for infrastructure security, ranging from recovery of the costs of prudently incurred transmission infrastructure investments to encouraging infrastructure security investments. Staff has engaged with utilities to encourage voluntary infrastructure security investments and implementation of best practices for cybersecurity measures.

Under the Commission’s ratemaking authority, the Commission has authorized utilities with formula rates, for example, to recover prudently incurred costs related to “security and reliability” through formula rates.²⁴ Cybersecurity activities can be included in a wide range of accounting categories, which are then automatically flowed through and recovered in formula rates either as plant components within rate base or as expense line items of the formula rate, depending on the nature of the cost that the utility incurs. These costs include transmission plant (e.g., transmission line upgrades to harden the system), general and intangible plant (e.g., software, computers, and cybersecurity investments), operations and maintenance (e.g., computer hardware, software, substations, and transmission systems), and administrative and general line items (e.g., labor, associated personnel, and outside services). The ability to automatically recover prudently incurred investments in transmission infrastructure security as they are incurred provides a significant incentive for utilities to make such investments. In addition, the Commission has accepted utility proposals to recover security costs as part of utilities’

²³ Defense-in-depth is “[t]he application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.” NIST, *Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/defense_in_depth.

²⁴ See *Boston Edison Co.*, 109 FERC ¶ 61,300, at P 40 (2004) (accepting proposed modifications to transmission formula rates filed by Boston Edison Company to allow recovery of capitalized software costs that the utility stated it incurred to comply with the Commission’s mandate to safeguard the reliability and security of its transmission system), *order on reh’g*, 111 FERC ¶ 61,266 (2005).

stated rates.²⁵

The Commission has taken a variety of actions designed to more specifically incent infrastructure security. On September 14, 2001, days after the terrorist attacks of September 11, 2001, the Commission issued a policy statement in which it recognized that “electric, gas, and oil companies may need to adopt new procedures, update existing procedures, and install facilities to further safeguard their electric power transmission grid and gas and oil pipeline systems.”²⁶ The Commission stated that it would “approve applications to recover prudently incurred costs necessary to further safeguard the reliability and security of our energy supply infrastructure.”²⁷ The Commission also noted that companies could propose a separate rate recovery mechanism, such as a surcharge to currently existing rates or some other cost recovery method, for such costs.²⁸

In addition, the Commission has authorized programs to enhance security through transmission equipment sharing. For example, in 2006, the Commission approved a proposal designed to increase the industry's inventory of spare electric transformers and provided related incentives. A group of investor-owned utilities developed a Spare Transformer Sharing Agreement (STEP Agreement) intended to “ensure that the electric industry has sufficient capability to restore service in the event of coordinated, deliberate destruction of utility substations.”²⁹ The Commission's order provided for blanket authorization under FPA section 203³⁰ for any of the STEP Agreement's signatories to be permitted to transfer transformers under the STEP Agreement.³¹ To encourage participation in the STEP Agreement, the Commission also found that participation in the STEP Agreement was prudent, the costs of participation qualified for single-issue rate treatment, and accorded all future jurisdictional signatories to the STEP Agreement the

²⁵ See *Pac. Gas and Elec. Co.*, 149 FERC ¶ 61,112 (2014); *Pac. Gas and Elec. Co.*, 146 FERC ¶ 61,034 (2014).

²⁶ *Extraordinary Expenditures Necessary to Safeguard Nat'l Energy Supplies*, 96 FERC ¶ 61,299, at 62,129 (2001).

²⁷ *Id.*

²⁸ *Id.* See also *Boston Edison*, 109 FERC ¶ 61,300 at P 40; *Policy Statement on Matters Related to Bulk Power Sys. Reliability*, 107 FERC ¶ 61,052 (2004).

²⁹ *Edison Elec. Inst. on behalf of the Jurisdictional Signatories to the Spare Transformer Sharing Agreement*, 116 FERC ¶ 61,280, at P 2 (2006) (STEP Order).

³⁰ 16 U.S.C. § 824b (2018).

³¹ STEP Order, 116 FERC ¶ 61,280 at P 21.

same benefits as current signatories.³²

With respect to single-issue ratemaking, typically, when a utility files to change its rates pursuant to FPA section 205, the Commission considers the utility's total cost of providing service in the Commission's determination of a just and reasonable rate. Thus, the Commission's regulations generally require a utility seeking a rate increase to file a comprehensive cost-of-service study on all of its transmission costs, rather than focus on just a single or limited component(s) of the utility's rate.³³ To encourage investment in critical transmission infrastructure security, the Commission has indicated its willingness to waive its regulations and allow a utility to request a selective adjustment to recover costs associated with an incremental transmission line or upgrade or an incremental component of a transmission line (such as a change to return on equity or requests for financial transmission investment incentives).³⁴

The Commission has also examined maintaining the security and reliability of energy infrastructure and how to provide incentives and cost recovery for security investments in energy infrastructure. On March 28, 2019, the Commission and the United States Department of Energy convened a technical conference to discuss current cyber and physical security practices used to protect energy infrastructure and to explore how federal and state authorities can provide incentives and cost recovery for security investments in energy infrastructure, particularly for the electric and natural gas sectors. Specifically, the technical conference was aimed at better understanding: (1) the types of cyber and physical security threats to energy infrastructure, particularly electric transmission, generation, and natural gas pipelines; (2) the need for security investments that go beyond those measures already required by mandatory reliability standards, including in infrastructure not subject to those standards (e.g., natural gas pipelines); (3) how the costs of such investments are or could be recovered; and (4) whether additional incentives for making such investments are needed, and, if so, how those incentives should be designed.³⁵

³² *Id.* P 43. See also *Jurisdictional Reg'l Equip. Sharing for Transmission Outage Restoration Participants*, 163 FERC ¶ 61,005, at P 2 (2018).

³³ Commission regulations on electric rates charged to wholesale electric transmission customers are included in 18 C.F.R. Part 35.

³⁴ See, e.g., Order No. 679, 116 FERC ¶ 61,057, at P 192, *order on reh'g*, Order No. 679-A, 117 FERC ¶ 61,345 (2006), *order on reh'g*, 119 FERC ¶ 61,062 (2007) ("[A]pplicants filing for single-issue ratemaking for a particular project . . . will be required to fully develop and support any transmission rate designed to recover the costs of a particular transmission system facility or upgrade The Commission will consider the potential need to combine or reconcile the new rate with any existing transmission rate when an applicant submits a request for incentives.").

The topic of how to incent cybersecurity was also addressed in July 2018 and June 2019 reliability technical conferences convened by the Commission. The July 31, 2018, *2018 Reliability Technical Conference* included a panel discussion on “Addressing the Evolving Cybersecurity Threat.”³⁶ The June 27, 2019, *2019 Reliability Technical Conference* examined topics that included adoption of cloud-based computer services and virtualization technologies by utilities in a manner that addresses security concerns.³⁷

Finally, staff conducts voluntary security assessments for utilities to identify threats and vulnerabilities to their energy infrastructure facilities and networks. This engagement allows the development of best practices to encourage these utilities to voluntarily make security changes that may involve additional investments to better protect critical transmission infrastructure security. Utilities have an opportunity for cost recovery for such investments.

B. The Need for Cybersecurity Investment

As discussed above, the Commission has employed both FPA section 215 and its other statutory authority to address cybersecurity across jurisdictional facilities. To date, FPA section 215 and the CIP Reliability Standards promulgated under that section have served as the Commission’s primary tool for driving changes to cybersecurity practices within the electric sector.

While the CIP Reliability Standards form an effective technical baseline for cybersecurity practices, they have certain limitations. For instance, the Reliability Standards do not necessarily require entities to employ best practices.³⁸ Moreover, the standards development process does not lend itself to addressing rapidly evolving cybersecurity threats. It can take many months for a new standard to be developed, and once approved, it may be several more months or years before fully implemented and enforceable.³⁹ Since cybersecurity threats can adapt and spread quickly, attackers can use

³⁵ See FERC, *FERC/DOE Security Investments for Energy Infrastructure Technical Conference*, Final Agenda, Docket No. AD19-12-000, at 1 (filed April 2, 2019).

³⁶ FERC, *2018 Reliability Technical Conference*, Final Agenda, Docket No. AD18-11-000, at 5 (Aug. 2, 2018).

³⁷ FERC, *2019 Reliability Technical Conference*, Final Agenda, Docket No. AD19-13-000, at 2-3 (June 27, 2019).

³⁸ Order No. 672, 114 FERC ¶ 61,104 at P 328.

³⁹ See, e.g., Am. Elec. Power, Inc., Comments, Docket No. PL19-3-000, at 13-14 (June 26, 2019) (noting that there is a potential gap between the dynamic threats faced by

sophisticated methods to exploit the interdependency of connected networks and equipment and target facilities, some of which may not be covered under the standards. Further, these growing threats come at a time of great change in the operation of the transmission system in which the number of attack vectors is increasing.⁴⁰ The standards development process, while inclusive and deliberative, is also public, potentially providing information to adversarial entities regarding limits and preferred approaches to implementation. Also, because the CIP Reliability Standards apply to BES facilities, which are generally 100 kV or higher as identified in CIP-002, not all operational technology is covered by these standards. Therefore, while cybersecurity systems that are not subject to the CIP Reliability Standards may be less critical to reliable operations, compromise of these systems may allow access to more critical systems.

In addition, changes to the operating environment can occur suddenly and without warning, such as under the COVID-19 national emergency. As the power sector is adapting to expanded remote operations, there is the potential for increased vulnerabilities and potential amplification of the effect of cybersecurity threats to the BES. Therefore, it is important that utilities have the ability to make cybersecurity investments to quickly and effectively adapt to address unforeseen circumstances.

For these reasons, this staff paper discusses augmenting the current CIP Reliability Standards under FPA section 215 with an incentive-based approach under FPA section 219 that encourages utilities to undertake cybersecurity investments on a voluntary basis. This approach would incentivize a utility to adopt best practices to protect its own transmission system as well as improve the security of the BES. Further, it could allow the industry to be more agile in monitoring and responding to new and (un)anticipated 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 utility to tailor its request for incentives to the potential challenges and responsive actions that it faces. In the future, these voluntary actions taken by utilities, if proven beneficial, could be the basis of future CIP Reliability Standards that are mandatory.

IV. Incentives Framework for Cybersecurity Investment

Providing transmission incentives for cybersecurity investments will require the

the energy industry and the CIP Reliability Standards development and compliance process, which sets the rules for minimum compliance).

⁴⁰ See, e.g., Eversource Energy Serv. Co., Comments, Docket No. PL19-3-000, at 29-30 (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).

Commission to establish a new framework for evaluating requests for transmission incentives by utilities for cybersecurity investments. As discussed above, augmenting the current CIP Reliability Standards with an incentive-based approach under FPA section 219 that encourages utilities to undertake cybersecurity investments on a voluntary basis may have significant benefits. However, a first necessary step is to establish approaches that examine the effectiveness of cybersecurity investments in enabling the utility to achieve a level of protection that exceeds the CIP Reliability Standards but also enhances the security of its transmission system. A utility will then be able to identify the cybersecurity investments for which it seeks transmission incentives. The Commission then can evaluate such transmission incentive requests. This section discusses how the typical suite of ratemaking incentives awarded to transmission projects could apply in the context of cybersecurity and two potential approaches for determining which cybersecurity investments warrant incentives.

A. Description of Incentives for Cybersecurity Investments

Incentives for cybersecurity investments could include both non-ROE and ROE incentives. With respect to the non-ROE incentives, cybersecurity investments could be eligible for Construction Work in Progress, recovery of abandoned plant costs, and accelerated depreciation.⁴¹ These incentives could reduce the financial risk associated with additional investments in cybersecurity, as they do for major transmission projects. For example, the Construction Work in Progress incentive can mitigate cash flow concerns caused by the increased expenditures associated with undertaking cybersecurity upgrades by allowing a return on investments during the construction period and before they are placed in service. However, these incentives may be less beneficial in this context than for major transmission investments, given the much faster deployment of cybersecurity upgrades and the significantly lower capital requirements compared to transmission projects. Similarly, there may be a relatively short depreciation life for most cybersecurity investments, and thus, it is unclear whether providing accelerated depreciation will have a substantial impact on cost recovery.

ROE incentives would apply only to the specific incremental cybersecurity investments identified in an applicant's filing. However, applying an ROE incentive only to the specific incremental cybersecurity investment by the utility may fail to provide a meaningful incentive for the cybersecurity investment given the relatively low capital cost of cybersecurity projects. There may be other ways to implement an ROE incentive

⁴¹ A hypothetical capital structure incentive may not be warranted for cybersecurity investments. Because cybersecurity investments tend to be small compared to major transmission projects, cybersecurity investments are unlikely to materially affect the overall capital structure of utilities during the construction/deployment period.

under the FPA that provides a meaningful incentive for cybersecurity investments and that would be just and reasonable. Staff seeks comment on this issue.

In limited circumstances, the Commission could consider allowing a utility to defer certain costs that have traditionally been categorized as expenses under the Commission's accounting standards and recovered through rates as expenses. Certain cost categories, such as software, that companies traditionally purchase and could capitalize, are now often procured as services with periodic payments to vendors for lease of software that is updated as needed. Therefore, to encourage investment in cybersecurity, the Commission could consider allowing utilities to defer and amortize eligible costs that are typically recorded as expenses that are associated with third-party hardware, software, and computing and networking services over a shorter period (such as five years).

B. Approaches to Identify Cybersecurity Investments Eligible for Incentives

In order to determine whether a utility's cybersecurity investments are eligible for incentives, the Commission would need to develop an approach for identifying the cybersecurity investments that it seeks to incentivize. This staff paper proposes two potential approaches.

Under both approaches, utilities could be eligible for incentives under FPA section 219 for voluntary cybersecurity investments that exceed the CIP Reliability Standards. Investments made to comply with the mandatory CIP Reliability Standards would not be eligible for incentives.

The first approach is based on a 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 is based on a utility voluntarily implementing portions of the cybersecurity framework developed by the National Institute of Standards and Technology (NIST). Both of these potential approaches, along with a potential process to apply the incentive, are discussed in sections below. The two approaches could be utilized independently or in combination.⁴²

⁴² Under this potential approach, although a utility could request a combination of incentives for its facility containing multiple assets, each individual asset is eligible for only one cybersecurity incentive at a time.

1. Incentives Based on Applying the CIP Reliability Standards to Additional Facilities

Under this approach, the Commission could provide a utility an ROE adder or other incentive for voluntarily applying certain CIP Reliability Standards to facilities that are not currently subject to those requirements. Specifically, under this approach, the utility would voluntarily apply the requirements for medium (or high) impact systems to low impact systems, and/or the requirements for high impact systems to medium impact systems. Using the existing NERC Reliability Standards as a framework for providing cybersecurity incentives has the benefit of allowing the Commission to leverage an existing set of baseline cybersecurity requirements. Further, utilities and the Commission are already familiar with the CIP Reliability Standards framework and applying known standards to additional facilities could be a straightforward way to establish a benchmark for determining whether the investment could warrant an incentive.

As discussed above, CIP-002 (Bulk Electric System Cyber System Categorization) is a foundational standard that requires a registered entity to categorize its cyber systems in terms of low, medium, and high impact to the grid. These impact ratings determine which requirements in NERC Reliability Standards CIP-004 through CIP-013 apply to BES Cyber Systems. Approximately 15% of currently effective CIP-004 through CIP-011 Reliability Standards requirements apply to low impact BES Cyber Systems.⁴³

CIP Reliability Standards version 5 became enforceable for high and medium impact BES Cyber Systems on July 1, 2016,⁴⁴ and the CIP Reliability Standards applicable to low impact BES Cyber Systems became enforceable on April 1, 2020. In approving the CIP Reliability Standards version 5, the Commission determined “that categorizing BES Cyber Systems based on their Low, Medium, or High Impact on the reliable operation of the bulk electric system, 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 cyber security controls improve the security posture of responsible entities.”⁴⁵

Under this approach, a utility could be eligible for an incentive for capital expenditures on BES Cyber Systems incurred to apply the CIP Reliability Standards requirements for higher impact assets to low or medium impact assets effective at the

⁴³ Summaries of the requirements and the applicability for low, medium and high impact BES Cyber Systems are available in the Appendix.

⁴⁴ See Order No. 791, 145 FERC ¶ 61,160.

⁴⁵ *Id.* P 2.

time of the investment.⁴⁶ By providing this incentive, the Commission could encourage utilities to increase the number of facilities that are protected by the requirements for medium and high impact BES Cyber Systems therefore improving the utility's security posture.

This staff paper identifies two potential methods the Commission could use to determine whether a utility is voluntarily applying the requirements of the CIP Reliability Standards to additional facilities:⁴⁷

- **Med/High Method:** This method would involve the utility implementing medium or high impact CIP Reliability Standards security controls for facilities identified as low or medium impact BES Cyber Systems.

Under the Med/High Method, a utility seeking a cybersecurity incentive for a particular facility that is classified as a low impact BES Cyber System would invest in ways to make that facility meet all the requirement and sub-requirement protections applicable to medium or high impact BES Cyber Systems, and invest in a facility classified as a medium impact BES Cyber System to make that facility meet all the requirement and sub-requirement protections applicable to high impact BES Cyber Systems. The 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 could receive incentives only for the investments it made to apply the more stringent protections.

- **Hub-Spoke Method:** This method would involve the utility applying the CIP Reliability Standards at locations containing low impact BES Cyber Systems by ensuring all external routable connectivity⁴⁸ to and from the low impact system must pass through a high or medium impact BES Cyber System. Specifically, all the cyber communications to and from a low impact system must come from a

⁴⁶ This is consistent with NERC's statement that "[e]ven in cases involving low-impact BES assets, an entity should strive for good cyber security policies and procedures" by considering adopting security controls for low impact BES Cyber Systems above those required under the CIP Reliability Standards. See NERC, *Lesson Learned Risks Posed by Firewall Firmware Vulnerabilities*, at 2-3 (Sept. 4, 2019), https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.

⁴⁷ The proposals are only examples. If the Commission adopts an incentive for voluntarily exceeding CIP Reliability Standards, it may consider other alternatives.

⁴⁸ External routable connectivity is 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 at 13.

medium or high impact BES Cyber System. Therefore, the cyber communication would be protected at a higher level before being transmitted to the low impact BES Cyber System.

Low impact BES Cyber Systems employing the Hub-Spoke Method would inherit the security benefit of either the medium or high impact controls.⁴⁹

Utilities that choose to implement the Med/High Method, the Hub-Spoke Method, or a combination of both could receive a rebuttable presumption that the investments provide significant benefits to merit up to a 200-basis point ROE incentive adder for such cybersecurity investments. Where equipment or software for such upgrades is leased, rather than purchased, utilities could request treatment of such investments as a regulatory asset, rather than expensing the cost, and depreciate such assets over five years.

Under this approach, if subsequent to the Commission granting the incentive, a utility became non-compliant with the CIP Reliability Standards to which they are voluntarily subjecting their facilities, the utility would not be subject to penalties. However, a utility would not be able to collect the incentive for the period of non-compliance and therefore would need to demonstrate compliance to continue to receive the incentive. Further, the utility would need to continue to comply with all of the mandatory NERC obligations for its low impact BES Cyber Systems.

Additionally, because the criteria for providing incentives would be tied to the CIP Reliability Standards as they exist at the time of the investment, the Commission's determination of the types of cybersecurity incentives that a utility is eligible for will reflect the existing version of the CIP Reliability Standards at the time of the utility's request for incentives. Staff recognizes that, given the amount of time it takes for NERC to develop a Reliability Standard and for the Commission to approve it, a potential CIP Reliability Standard that increases the requirements for a low or medium impact system to those of a medium or high impact system may take a year or longer to become enforceable. During this time, staff believes that a utility should be able to apply for an incentive for voluntarily applying the effective CIP Reliability Standards to facilities that are not covered at the time of the investment.

2. Incentives Based on the National Institute of Standards and Technology Cybersecurity Framework

Another approach would be to base the eligibility for incentives on a framework other than the CIP Reliability Standards, specifically the cybersecurity framework

⁴⁹ The Appendix includes a summary of the relevant currently effective CIP Reliability Standards and their associated impact levels.

developed by NIST (NIST Framework).⁵⁰ This approach would still consider the CIP Reliability Standards as a basis for granting cybersecurity incentives, while allowing utilities to employ alternative approaches to assessing risk under the NIST Framework. It would also offer the flexibility of non-prescriptive implementation options to encourage utilities to exceed the CIP Reliability Standards. Also, the NIST Framework is based on and updated with cybersecurity best practices and is consistent with other federal cybersecurity risk management initiatives for the 16 U.S. critical infrastructure sectors. This approach could allow incentives to be applied to more facilities which are beyond the BES Cyber Systems in the CIP Reliability Standards.⁵¹ Thus, under this approach, the Commission could utilize the NIST Framework to evaluate whether cybersecurity investments that exceed CIP Reliability Standards are eligible for incentives. An open question would be whether eligible facilities include any asset directly connected to the transmission system, or other assets such as portions of the corporate network that can impact the cybersecurity of these systems.

Executive Order No. 13636⁵² required development of the NIST Framework to “provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.”⁵³ In an August 2019 report,⁵⁴ the Government Accountability Office noted that the NIST Framework “provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across all critical infrastructure sectors, including the energy sector” and is a “voluntary, risk-based cybersecurity framework [that] comprises a set of

⁵⁰ NIST is a part of the U.S. Department of Commerce that advances measurement science, standards, and technology. It has developed a voluntary Framework for Improving Critical Infrastructure Cybersecurity to “address and manage cybersecurity risk in a cost-effective way based on business and organizational needs without placing additional regulatory requirements on businesses.” NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, at v (Apr. 16, 2018), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

⁵¹ This approach is also broad-based and allows for rapid changes to address sudden and unforeseen circumstances.

⁵² *Improving Critical Infrastructure Cybersecurity*, 77 Fed. Reg. 11,739 (Feb. 19, 2013).

⁵³ *Id.* at 11,741.

⁵⁴ U.S. Gov’t Accountability Office, *Critical Infrastructure Protection – Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid* (Aug. 2019), <https://www.gao.gov/assets/710/701079.pdf>.

industry standards and best practices to help organizations manage cybersecurity risks.”⁵⁵ The NIST Framework is based on the categories and subcategories of five overarching cybersecurity functions – Identify, Protect, Detect, Respond, and Recover. There are 23 categories within those functions and 108 sub-categories. Below, staff identifies five distinct types of security controls within this structure that may be considered for incentives.⁵⁶

Under this approach, the Commission could grant incentives for implementing certain security controls included in the NIST Framework. Although the NIST Framework contains many types of security controls, the Commission could consider limiting eligibility for incentives to the types of controls that appear most likely to provide a significant benefit to the cybersecurity of FERC-jurisdictional transmission facilities, not just the BES. These five types of controls represent the majority of security controls included in the NIST Framework and include the following: (1) automated and continuous monitoring; (2) access control; (3) data protection; (4) incident response; and (5) physical security of cyber systems.⁵⁷ Given the continuous and rapid changes of cybersecurity risks, the Commission may need to periodically update the types of security controls eligible for incentives. As discussed below, utilities seeking an incentive under this approach would need to show how a cybersecurity investment, e.g., 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 utility to meet NIST Framework security controls, as identified above, and also how the cybersecurity investment would exceed the requirements of the CIP Reliability Standards.

An installation of a dynamic asset management program to improve a utility’s ability to quickly detect and address new or previously unknown equipment on its network is an example of a cybersecurity investment that may be eligible for an incentive under the automated and continuous monitoring security control type.⁵⁸ Unknown and

⁵⁵ *Id.* at 4, 12.

⁵⁶ 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.

⁵⁷ In contrast, controls focused on documentation and planning, such as training, development of plans, guides, playbooks, are less likely to provide significant benefits to the transmission system and therefore may not warrant incentives.

⁵⁸ In the NIST Framework, Dynamic Asset Management can be found within the Identify (ID) Function in the Asset Management Category (ID.AM) which states: “The

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 and block any unauthorized access. This is an enhancement that is not currently covered by the CIP Reliability Standards but is recommended by the NIST Framework and could offer cybersecurity benefits to the transmission system.

Another example that may be applicable under the identified NIST Framework security control type of automated and continuous monitoring would be implementation of a dynamic file analysis program or a “sandbox.”⁵⁹ A sandbox can be described as an advanced malware detection environment for the corporate email system. Any attachment or weblink is stripped from the email and dropped into the sandbox. In simple terms, a sandbox is an isolated environment that mimics the end-user operating environment. Any malicious code deployed in the sandbox will 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 utility to the threat. The deployment of sandboxes enhances the ability of a utility to detect and prevent the delivery of malicious code, disrupt social engineering attacks on users, test software for dangerous behavior, and perform post-incident forensic triage and analysis. Putting this added layer of protection in place is an enhancement that is not required by the CIP Reliability Standards but is recommended by the NIST Framework and could offer cybersecurity benefits to the transmission system.

Under this approach, a utility could be eligible for an incentive if it demonstrates that its cybersecurity investment is consistent with the five types of NIST Framework controls identified in this paper, exceeds the requirements of the CIP Reliability

data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.” Within the Asset Management category, this can be further defined by subcategory ID.AM-1: “Physical devices and systems within the organization are inventoried” and subcategory ID.AM-2: “Software platforms and applications within the organization are inventoried.” NIST, *Cybersecurity Framework*, at 20 (Feb. 12, 2014), <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

⁵⁹ In the NIST Framework, Automated and Continuous Monitoring can be found within the Detect (DE) Function in the Security Continuous Monitoring Category (DE.CM) which states: “The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.” Within this category, this can be further defined by subcategory DE.CM-1: “The network is monitored to detect potential cybersecurity events.” *Id.* at 30.

Standards, and provides significant cybersecurity benefits to Commission-jurisdictional transmission facilities. While the administrative burden associated with this approach is not expected to be prohibitive, the Commission could also consider establishing a rebuttable presumption of significant benefits for certain types of investments that follow the NIST Framework to streamline the application process.

Finally, as the Commission evaluates incentive applications, it will need to remain cognizant of ongoing changes to the CIP Reliability Standards, the NIST Framework, or underlying referenced security controls.

C. Application Process

To obtain a cybersecurity incentive, a utility in its application would need to provide sufficient information for the Commission to determine whether the investment merits an incentive. Given the highly technical nature of cybersecurity, security considerations associated with cybersecurity matters, and the differences between cybersecurity investments and other more capital-intensive investments that generally receive incentive rates, applications for cybersecurity incentives and the Commission’s process for evaluating such applications would likely be substantially different than the processes the Commission uses to evaluate other requests for transmission incentives. Below, this staff paper proposes elements that may need to be included in any application for incentives by a utility for cybersecurity investments under either approach discussed above.

1. Incentives Based on Applying the CIP Reliability Standards to Additional Facilities

The incentive application would include a description of the cybersecurity investments, the CIP Reliability Standards requirements that were voluntarily applied to facilities not covered by the requirements and where (if it is not applied across the whole CIP environment), anticipated completion date, and anticipated cost.⁶⁰ Because the Med/High and Hub-Spoke Methods are based on the CIP Reliability Standards that have already been approved by the Commission, an applicant would not need to describe how such investments improve cybersecurity or are specifically tailored for the utility, but rather an applicant would need to demonstrate that the low impact systems fully comply with the CIP Reliability Standard requirements for medium or high impact systems, and medium impact systems fully comply with requirements for high impact systems. Under this approach, a specific showing of benefits would not be necessary for each filing

⁶⁰ Consistent with other transmission incentives approved under FPA section 219, costs for cybersecurity projects and their associated incentives will be recovered in a utility’s rates consistent with the utilities’ transmission rate protocols.

because both the Med/High and Hub-Spoke Methods would result in a significant increase in the required security controls. Specifically, approximately 15% of currently effective CIP-004 through CIP-011 Reliability Standards requirements apply to low impact BES Cyber Systems. By increasing the BES Cyber System protections for low impact to medium or high impact, BES Cyber Systems will increase the protections by several magnitudes. Thus, a utility that makes these showings will be presumed to be eligible for the incentive.

2. Incentives Based on the NIST Framework

The utility's request for incentives for cybersecurity investment would include a description of the cybersecurity investments; how they meet the five types of NIST Framework controls identified in this paper; how they resulted in significant cybersecurity benefits for Commission-jurisdictional transmission facilities; how they exceed the CIP Reliability Standards requirements, including whether they addressed any differences; anticipated completion date of the investment; and anticipated cost.

D. Magnitude of the Incentive(s)

Utilities could be eligible for up to 200 basis points of ROE incentive for cybersecurity investments. This amount could incent additional cybersecurity investments without being unduly burdensome for ratepayers. While this would be higher than the project specific-ROE incentives proposed in the Transmission Incentives NOPR, incentives in the context of cybersecurity are distinguishable because the investments contemplated here are significantly smaller than most transmission projects and are recovered over a shorter time horizon. Moreover, all ROE incentives for cybersecurity investment could be subject to a sunset date to further reduce the potential impact to ratepayers.

E. Sunset/Modification Provision of the Incentive(s)

Given the quickly evolving nature of cybersecurity threats and best practices, it may be appropriate to require that applicants include a sunset date for all cybersecurity incentives. In light of these factors, this paper proposes that incentivized cybersecurity investments should have a sunset date of no more than three to five years. While requiring a sunset date would stand in contrast to the Commission's treatment of incentives for other investments, there are significant differences between cybersecurity investments and other incentives that the Commission has granted. For example, investments in high voltage transmission lines are extremely capital intensive and are generally expected to produce benefits over a long-time horizon. On the other hand, because of the rapidly changing cybersecurity environment, cybersecurity investments

can become obsolete or provide significantly reduced value in a comparatively short time. Moreover, continued evolution of the mandatory reliability standards may result in certain practices that were once voluntary becoming mandatory.

There is a possibility that certain cybersecurity practices may become mandatory before an incentive's sunset date. Given this possibility, the Commission could consider allowing recipients of such incentives to retain the authorized incentive treatments for the specific investments until the earlier of the sunset date or the date when such investments subsequently become mandatory. In addition, there may also be a situation where NERC is either exploring or actively developing a new CIP Reliability Standard but has not yet received final Commission approval. Staff seeks comment on whether there is a point in this process at which the Commission should no longer grant incentives for investments covered by the possible standard.

F. Information Confidentiality

In order to demonstrate eligibility for cybersecurity incentives applicants need to provide detailed information, as discussed above. Depending on the detail provided in applications, this information may be sensitive or otherwise confidential and applicants may want to limit disclosure of this information to third parties. The cybersecurity incentives policy must balance the needs of confidentiality of cybersecurity systems and protocols and the need for transparency in rates when awarding incentive rates to utilities for cybersecurity investments. The Commission balances these considerations through its confidential⁶¹ and Critical Energy/Electric Infrastructure Information (CEII) filing regulations.⁶² These regulations recognize that intervenors in a Commission proceeding

⁶¹ 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 C.F.R. § 388.112 (2019).

⁶² 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 C.F.R. § 388.113.

to which a right of intervention exists, 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. Accordingly, if utilities are concerned that the information contained in an application for incentives could lead to the disclosure of confidential information or CEII related to their cybersecurity systems, an applicant could file its application pursuant to these procedures. However, as discussed above, this could allow for intervenors to access the confidential information or CEII contained in the application after the signing of a protective agreement with the applicant.⁶³

G. Potential Reporting Requirements

Given the unique nature of cybersecurity requirements, additional reporting requirements for cybersecurity incentives will be needed in addition to those required under FERC Form No. 730. In the Transmission Incentives NOPR, the Commission proposed to require that utilities continue to provide certain data, projections, and related information to ensure that existing incentives are successfully meeting the objectives of FPA section 219.⁶⁴ It is expected that the reporting requirements for cybersecurity investments would likely differ from those of traditional transmission investments. One approach to reporting would be to require a utility that receives a cybersecurity incentive to file an annual informational filing and be subject to audits.

Just as the Commission has proposed increased informational reporting for transmission investments for incentive recipients through Form No. 730, it will be important for recipients to describe the nature and cost of cybersecurity investments. Such informational filings should be through separate filings than the Form No. 730, given the greater confidentiality considerations. Recipients of cybersecurity incentives would be required to make annual filings detailing the specific investments that were made pursuant to the Commission's approval and what FERC account they fall into. In such filings, the applicant would attest to the project's completion and entering into service, provide the actual cost for the project, and submit quantifiable metrics to support that the expected enhanced cybersecurity benefits were realized. In addition to providing equivalence in reporting requirements between cybersecurity investments and other

⁶³ 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 C.F.R. §§ 388.112(b)(2)(iv), 388.113(g)(4).

⁶⁴ Transmission Incentives NOPR, 170 FERC ¶ 61,204 at P 115.

transmission investments that receive incentives, the reporting requirements would address issues specific to cybersecurity investments. First, cybersecurity investments are not observable such that it is not readily apparent if and when such investments are completed and serving customers, making additional reporting requirements important to confirming their completion. Second, certain cybersecurity investments may require utilities to undertake subsequent actions or make expenditures to maintain the status for which they receive incentives. Annual reports enable utilities to demonstrate such actions or expenditures.

For incentives where the Commission allows capitalization of expenses into regulatory assets, annual informational filings should describe such expenses in substantial detail to demonstrate that they are for expenses related to upgrades and not for ongoing services including system maintenance, surveillance, and other labor costs. The Commission could provide additional guidance in the future on the specific line items and informational requirements of such forms. Generally, such filings would be subject to protective agreements given their sensitive information.

Entities receiving incentives may also be subject to audit by the Commission's Office of Enforcement. Commission staff in the Office of Enforcement routinely conduct audits of accounting practices, such as FERC Form No. 1 annual filings to provide reasonable assurance that entities are in compliance with relevant Commission regulations and orders. In the context of cybersecurity incentives, accounting audits could focus on whether utilities are appropriately deferring only eligible expenses for either the CIP Reliability Standards or NIST Framework approaches. Further, oversight audits can confirm not only that investments are actually made but that the utility is operating its system and taking other actions that are required for cybersecurity investments to be effective. Alternatively, approved third parties could conduct such audits, although, in that case, the Commission would need to develop protocols to ensure that such audits are impartial and accurate.

V. Request for Comments

This staff paper identifies issues for the Commission's consideration as it further evaluates providing incentives to utilities for cybersecurity investments based on staff's outreach and expertise. This staff paper also sets forth two potential approaches the Commission could use to evaluate whether certain cybersecurity investments qualify for transmission incentives. Interested parties are invited to file comments on the matters addressed in this staff paper, the questions below, and any additional approaches for structuring an incentive for cybersecurity investments not explored in this staff paper. Comments are due within 60 days of the issuance of this paper and reply comments within 75 days of the issuance of this paper.

1. Should the Commission consider adopting one or both of the CIP Reliability

Standards and NIST Framework approaches? Describe any other possible approach in detail.

2. Are the methods for granting incentives based on the CIP Reliability Standards (Med/High and Hub-Spoke Method) adequate? What steps should the Commission consider taking to ensure the incentive eligibility and corresponding application evaluation processes are clear and fair? What other types of cybersecurity investment based on the CIP Reliability Standards should be eligible for the incentive? Describe in detail the other types of cybersecurity investment based on the CIP Reliability Standards and how they would enhance cybersecurity.
3. Should the Commission provide a rebuttable presumption of the reasonableness and thus the applicability of incentives for some or all investments in either the Med/High or the Hub-Spoke Method?
4. Is the proposed approach for granting incentives based on the NIST Framework adequate? What steps should the Commission consider taking to ensure the incentive eligibility and corresponding application evaluation processes are clear and fair? What type of incentive would encourage cybersecurity improvements based on the NIST Framework? Should the incentives be available to incremental cybersecurity measures applied to both operational technology and corporate network information technology systems?
5. Which components of the NIST Framework should be considered for an incentive? What type of guidance should the Commission provide on which components of the NIST Framework merit incentive? How might an entity demonstrate the cybersecurity expenditures that qualify under the NIST Framework?
6. Recognizing that FPA section 219 applies incentives to investments for the transmission of electric energy in interstate commerce that result in certain benefits, to what extent can investments in other systems directly connected to the transmission system, or other assets such as portions of the corporate network that can impact the cybersecurity of these systems qualify for incentives? Where investments are enterprise-wide and not transmission-specific, would providing an incentive on the portion allocated to transmission provide a material incentive?
7. Is a 200-basis point project-specific ROE adder enough to materially incent cybersecurity investments that exceed the requirements of the CIP Reliability Standards? If not, what size basis point ROE incentive adder would be adequate to incentivize such cybersecurity investments? If project-specific ROE adders are not sufficient, are there other approaches that the Commission could take with respect to ROE adders that would incent the desired cybersecurity investments?

8. What, if any, guidance should the Commission provide on how to structure an application for cybersecurity incentives? Describe in detail what criteria the Commission could use when evaluating an application for cybersecurity incentives.
9. Would the documentation requirements of the two approaches described above require disclosure of confidential information or CEII or would applicants be able to make the suggested showings without disclosing confidential information or CEII? If so, would the requirement to provide this information subject to disclosure to intervenors under a protective agreement discourage applications for cybersecurity incentives?
10. How can the Commission verify that actions associated with the incentive are complete and maintained? Should the applicant be required to submit a compliance filing once the work is completed or after an internal certification process or audit is completed? If a third-party auditor is chosen, what criteria should the third-party have to use to ensure proper verification?
11. Given the rapidly changing cybersecurity environment, should the Commission adopt a sunset date of three to five years for certain incentivized cybersecurity investments? At what point in the timeline between NERC announcing that it is exploring a new standard and final Commission approval, should the Commission no longer accept new applications for incentives for such investments?

Appendix – CIP Reliability Standards Impact-Level Summary

The following table includes a summary of the relevant currently effective CIP Reliability Standards requirements and their associated impact levels. The Hub-Spoke Method applied to low impact BES Cyber Systems would inherit the security benefit of either the medium or high impact controls. While a requirement might apply to BES Cyber Systems of both medium and high impact systems, the specific sub-requirements under each standard may not apply to both medium and high impact systems.

Standard	Req	Description	Low	Medium	High
CIP-002-5.1a	R1	Identify BES Cyber Systems	X	X	X
CIP-002-5.1a	R2	15 Month Review of R1	X	X	X
CIP-003-8	R1	CIP Policies with Sr. CIP Manager sign off	X	X	X
CIP-003-8	R2	Low Impact BES Cyber Systems	X		
CIP-003-8	R3	Identify a Sr. CIP Manager	X	X	X
CIP-003-8	R4	Delegations of authority by Sr. CIP Manager	X	X	X
CIP-004-6	R1	Security Awareness Program		X	X
CIP-004-6	R2	Cyber Security Training Program		X	X
CIP-004-6	R3	Personnel Risk Assessment Program		X	X
CIP-004-6	R4	Access Management Program (of BES Cyber Systems)		X	X
CIP-004-6	R5	Access Revocation Program (of BES Cyber Systems)		X	X
CIP-005-6	R1	Electronic Security Perimeter (i.e., firewalls, etc.)		X	X
CIP-005-6	R2	Interactive Remote Access Management		X	X

Standard	Req	Description	Low	Medium	High
CIP-006-6	R1	Physical Security Plan		X	X
CIP-006-6	R2	Visitor Control Program		X	X
CIP-006-6	R3	Physical Access Control Maintenance and Testing		X	X
CIP-007-6	R1	Ports and Services		X	X
CIP-007-6	R2	Security Patch Management		X	X
CIP-007-6	R3	Malicious Code Prevention		X	X
CIP-007-6	R4	Security Event Monitoring		X	X
CIP-007-6	R5	System Access Control		X	X
CIP-008-6	R1	Incident Response Plan		X	X
CIP-008-6	R2	Incident Response Implementation and Testing		X	X
CIP-008-6	R3	Incident Response Plan Review & Update		X	X
CIP-008-6	R4	Notifications and Reporting for Cyber Security Incidents		X	X
CIP-009-6	R1	Recovery Plan		X	
CIP-009-6	R2	Recovery Plan Implementation and Testing		X	X
CIP-009-6	R3	Recovery Plan Review & Update		X	X
CIP-010-3	R1	Configuration Change Management		X	X
CIP-010-3	R2	Configuration Monitoring			X
CIP-010-3	R3	Vulnerability Assessments		X	X
CIP-010-3	R4	Transient Cyber Assets and Removable Media		X	X
CIP-011-2	R1	Information Protection		X	X

Standard	Req	Description	Low	Medium	High
CIP-011-2	R2	BES Cyber Asset Reuse and Disposal		X	X