FERC-725B (OMB Control No. 1902-0248)
Proposed Rule (issued 12/17/2020) in Docket No. RM21-3-000
RIN: 1902-AF76

Supporting Statement for

FERC-725B (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards), as modified by the Proposed Rule in Docket No. RM21-3-000

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review the revisions to the FERC-725B information collection (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards) as implemented by the Notice of Proposed Rulemaking (issued 12/17/2020)[1] in Docket No. RM21-3-000.

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, Congress enacted the Energy Policy Act of 2005.[2] The Energy Policy Act of 2005 added a new section 215 to the FPA,[3] which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards,[4] 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.
On February 3, 2006, the Commission issued Order No. 672,[5] implementing FPA section 215. The Commission subsequently certified NERC as the Electric Reliability 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.[6] 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.

1 The Order is posted in FERC's eLibrary at https://elibrary.ferc.gov/eLibrary/filedownload?fileid=15682657.
2 Energy Policy Act of 2005, Pub. L. No. 109-58, sec. 1261 *et seq.*, 119 Stat. 594 (2005).
3 16 U.S.C. 824o.
4 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).
5 *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).
6 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."

On January 18, 2008, the Commission issued Order No. 706,[7] 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,[8] approving CIP version 5 Standards, the last major revision to the CIP Reliability Standards. The CIP version 5 Standards implement a tiered approach to categorize assets, identifying them as high, medium, or low risk to the operation of the Bulk Electric System (BES)[9] 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[10] are categorized as low impact systems. Most requirements in 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.[11]

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

---

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

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

9 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).

10 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, mis-operation, 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.

11 *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).

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:[12]

- 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 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 mis-operation or instability in the BES.
- CIP-004-6 Personnel and Training: requires entities to minimize the risk against compromise that could lead to mis-operation 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 mis-operation 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 mis-operation 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 mis-operation or instability in the BES.
- CIP-008-5 Incident Reporting and Response Planning:[13] 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.

12 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.
13 An update to CIP-008-6 Reliability Standard will become enforceable on January 1, 2021.

- 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 mis-operation 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 mis-operation or instability in the BES.
- CIP-012-1 Communications between Control Centers:[14] 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.

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.[15] The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.[16]

NOPR in RM21-3-000. On March 20, 2020, the Commission issued a Notice of Proposed Rulemaking on its transmission incentives policy under Federal Power Act section 219.[17] 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.[18]

2. HOW, BY WHOM, AND FOR WHAT PURPOSE THE INFORMATION IS TO BE USED AND THE CONSEQUENCES OF NOT COLLECTING THE INFORMATION

Pursuant to FPA sections 205 and 206, 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.

14 CIP-012-1: Communications between Control Centers will be subject to enforcement by July 1, 2022.
15 Order No. 822, 154 FERC ¶ 61,037 at 32.
16 Order No. 706, 122 FERC ¶ 61,040 at 72.
17 *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).
18 2019 Notice of Inquiry, 166 FERC ¶ 61,208 at P 5.

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 Commission's jurisdiction. 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. 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 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 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. We believe that this action is appropriate to facilitate increased cybersecurity investment, and that the resulting rates will be just and reasonable.

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.[19] We propose specific reporting requirements for each of the NERC CIP Incentives Approach and the NIST Framework Approach below.

The Transmission Incentives NOPR proposes additional reporting requirements for recipients of transmission incentives under FPA section 219.[20] 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

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

20 Transmission Incentives NOPR, 166 FERC ¶ 61,208 at P 115.

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 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.

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. 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. 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.

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.

3. **DESCRIBE ANY CONSIDERATION OF THE USE OF IMPROVED TECHNOLOGY TO REDUCE BURDEN AND TECHNICAL OR LEGAL OBSTACLES TO REDUCING BURDEN.**

The use of current or improved technology and the medium are not covered in Reliability Standards and are therefore left to the discretion of each respondent. We think that nearly all respondents are likely to make and keep related records in an electronic format. The compliance portals allow documents developed by the registered entities to be attached and uploaded to the Regional Entity's portal. Compliance data can also be submitted by filling out data forms on the portals. These portals are accessible through an internet browser password-protected user interface.
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.

4. DESCRIBE EFFORTS TO IDENTIFY DUPLICATION AND SHOW SPECIFICALLY WHY ANY SIMILAR INFORMATION ALREADY AVAILABLE CANNOT BE USED OR MODIFIED FOR USE FOR THE PURPOSE(S) DESCRIBED IN INSTRUCTION NO. 2

Filing requirements are periodically reviewed as OMB review dates arise or as the Commission may deem necessary in carrying out its regulatory responsibilities under the FPA in order to eliminate duplication and ensure that filing burden is minimized. There are no similar sources for information available that can be used or modified for these reporting purposes.

5. METHODS USED TO MINIMIZE BURDEN IN COLLECTION OF INFORMATION INVOLVING SMALL ENTITIES

The Commission estimates one-time and ongoing increases in reporting burden on variety of NERC-registered entities (including Reliability Coordinators, Generator Operators, Generator Owners, Interchange Coordinators, Transmission Operators, Balancing Authorities, Transmission Owners) due to the changes in the revised Reliability Standards, with no other increase in the cost of compliance (when compared with the current standards). Approximately 319 affected entities are expected to meet the SBA's definition for a small entity.[21]

The Reliability Standards do not contain provisions for minimizing the burden of the collection for small entities. All the requirements in the Reliability Standards apply to every applicable entity. However, small entities generally can reduce their burden by taking part in a joint registration organization or a coordinated function registration. These options allow an entity the ability to share its compliance burden with other similar entities. Detailed information regarding these options is available in NERC's Rules of Procedure at Section 1502, Paragraph 2, available at NERCs website.

6. CONSEQUENCE TO FEDERAL PROGRAM IF COLLECTION WERE

21 Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this Final Rule, we are using a 500-employee threshold due to each affected entity falling in the role of Electric Bulk Power Transmission and Control (NAISC Code: 221121).

CONDUCTED LESS FREQUENTLY

The consequences of not collecting the data associated with the Reliability Standard will result in an unmitigated risk from communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers of the NERC registered entities which operate the bulk electric system. Since the documentation is a plan to protect, not collecting the information and not having a plan will prevent the protection of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

FERC-725B information collection has no special circumstances.

8. DESCRIBE EFFORTS TO CONSULT OUTSIDE THE AGENCY: SUMMARIZE PUBLIC COMMENTS AND THE AGENCY'S RESPONSE TO THESE COMMENTS

The NOPR was published in the Federal Register on 2/05/2021 (86 FR XXXX), thereby providing public utilities and licensees, state commissions, Federal agencies, and other interested parties an opportunity to submit data, views, comments or suggestions concerning the proposed collections of data.

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

No payments or gifts have been made to respondents.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

NOPR in RM21-3-000. The Commission balances these considerations through its confidential and Critical Energy/Electric Infrastructure Information (CEII) filing regulations. 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. 18 CFR 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. 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.

CIP Reliability Standards. According to the NERC Rules of Procedure[22], "…a Receiving Entity shall keep in confidence and not copy, disclose, or distribute any Confidential Information or any part thereof without the permission of the Submitting Entity, except as otherwise legally required." This serves to protect confidential information submitted to NERC or Regional Entities.

Responding entities do not submit the information collected due to the Reliability Standards to FERC. Rather, they submit the information to NERC, the regional entities, or maintain it internally. Since there are no submissions made to FERC, FERC provides no specific provisions in order to protect confidentiality.

11. PROVIDE ADDITIONAL JUSTIFICATION FOR ANY QUESTIONS OF A SENSITIVE NATURE, SUCH AS SEXUAL BEHAVIOR AND ATTITUDES, RELIGIOUS BELIEFS, AND OTHER MATTERS THAT ARE COMMONLY CONSIDERED PRIVATE

This collection does not contain any questions of a sensitive nature.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

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.[23] 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. The Commission estimates that the NOPR would affect the burden[24] and cost[25] as follows:

22 Section 1502, Paragraph 2, available at NERCs website
23 The information requested is similar to the information FERC staff reviews during a NERC CIP Reliability Standards audit.
24 "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.
25 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).

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
FERC-725B - (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards) after adding filers from Cybersecurity Incentives Investment Activity (submitted as a separate IC within FERC-725B).					
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
Total			**223,895**		**2,044,626 hours; $169,703,958**

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 are like 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.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

There are no start-up or other non-labor costs.

Total Capital and Start-up cost: $0
Total Operation, Maintenance, and Purchase of Services: $0

All costs are due to this Final Rule are associated with burden hours (labor) and described in Questions #12 and #15 in this supporting statement.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The Regional Entities and NERC do most of the data processing, monitoring and compliance work for Reliability Standards. Any involvement by the Commission is covered under the FERC-725 collection (OMB Control No. 1902-0225) and is not part of this request or package. The data are not submitted to FERC.

The Commission does incur the costs associated with obtaining OMB clearance under the Paperwork Reduction Act (PRA). The PRA Administrative Cost is a Federal Cost associated with preparing, issuing, and submitting materials necessary to comply with the PRA for rulemakings, orders, or any other vehicle used to create, modify, extend, or discontinue an information collection. This average annual cost includes requests for extensions, all associated rulemakings and orders, other changes to the collection, and associated publications in the Federal Register.

FERC-725B	Number of Employees (FTEs)	Estimated Annual Federal Cost
Analysis and Processing of Filings	0	$0
Paperwork Reduction Act Administrative Cost [26]		$6,475
TOTAL		$6,475

15. REASONS FOR CHANGES IN BURDEN INCLUDING THE NEED FOR ANY INCREASE

In Order No. 822, the Commission directed NERC to, among other things, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communications links and sensitive bulk electric system data communicated

26 The Commission bases the cost of Paperwork Reduction Act administration on staff time, and other costs related to compliance with the Paperwork Reduction Act of 1995.

between bulk electric system Control Centers "in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." The Commission explained that Control Centers associated with responsible entities, including reliability coordinators, balancing authorities, and transmission operators, must be capable of receiving and storing a variety of bulk electric system data from their interconnected entities in order to adequately perform their reliability functions. The Commission, therefore, determined that "additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted."

A summary of the burden added to FERC-725B information collection due to the Final Rule in RM21-3-000 follows:

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	223,895	224,800	-925	20
Annual Time Burden (Hrs.)	2,044,626	2,119,709	-76,683	1,600
Annual Cost Burden ($)	$0	$0	$0	$0

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

There is no tabulating, statistical or publication plans.

17. DISPLAY OF THE EXPIRATION DATE

The expiration date is displayed in a table posted on ferc.gov at http://www.ferc.gov/docs-filing/info-collections.asp.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.