FERC-725B (OMB Control No. 1902-0248)
RIN: 1902-AG23
Final Rule published on July 2, 2025 (90 FR 28889)

Supporting Statement for:

**FERC-725B, Revisions in RM24-7, Critical Infrastructure Protection Reliability Standard CIP-015-1-Cyber Security-Internal Network Security Monitoring**

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review the revised collection of information designated as FERC-725B (Mandatory Reliability Standards: Critical Infrastructure Protection Reliability Standards) in RM24-7-000.

## 1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, The Electricity Modernization Act of 2005, which is Title XII of the Energy Policy Act of 2005 (EPAct 2005), was enacted into law. EPAct 2005 added a new section 215 to the Federal Power Act (FPA),[1] which provides that the Commission may certify an Electric Reliability Organization (ERO), the purpose of which is to establish and enforce Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[2] In 2006, the Commission certified the North American Electric Reliability Corporation (NERC) as the ERO pursuant to FPA section 215.[3]

**Reliability Standard CIP-015-1 (active)**
Proposed Reliability Standard CIP-015-1 is a new cybersecurity-related Reliability Standard requiring Internal Network Security Monitoring (INSM)[4] for Critical Infrastructure Protection (CIP) networked environments for all high impact bulk electric

1 16 U.S.C. 824o.
2 *Id*. 824o(e).
3 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on compliance*, 118 FERC ¶ 61,190, *order on reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir 2009).
4 INSM is "a subset of network security monitoring that is applied within a 'trust zone,' such as an electronic security perimeter." *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Order No. 887, 88 FR 8354 (Feb. 9, 2023), 182 FERC ¶ 61,021 at P 2 (2023).

system (BES)[5] Cyber Systems[6] with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. Proposed Reliability Standard CIP-015-1 will not apply to medium impact BES Cyber Systems without external routable connectivity.

**NERC Petition June 24, 2024**

The new standard, proposed by NERC, in June 2024, requires entities with BES facilities whose assets are designated high impact and medium impact with external routable connectivity to implement INSM for network traffic inside an electronic security perimeter to ensure the identification of anomalous network activity including an ongoing attack. High impact systems include large control centers. Medium impact systems include smaller control centers, ultra-high voltage transmission, and large substations and generating facilities.

---

5 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).

6 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.

Proposed Reliability Standard CIP-015-1 was developed in response to a Commission directive in Order No. 887. Order No. 887 was a final rule that directed NERC to develop new or modified CIP Reliability Standards requiring INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress."[7] The Commission, noting that INSM is "applied within a 'trust zone,' such as an electronic security perimeter," stated that for the final rule the applicable trust zone for INSM is the CIP-networked environment.[8]

Proposed Reliability Standard CIP-015-1 requires entities to implement INSM within the electronic security perimeter to close a reliability gap where vendors or individuals with authorized access in the CIP-networked environment are deemed trustworthy but could still introduce a cybersecurity risk. Requirement R1 of proposed Reliability Standard CIP-015-1 requires responsible entities to implement process(es) to monitor, detect, and evaluate anomalous activity in "networks protected by the Responsible Entity's Electronic Security Perimeter(s)" of high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity. Requirement R2 of proposed Reliability Standard CIP-015-1 requires responsible entities to implement process(es) for retaining INSM data associated with anomalous network activity as determined by the applicable responsible entities. Requirement R3 of proposed Reliability Standard CIP-015-1 requires responsible entities to implement process(es) to protect INSM monitoring data collected and retained in support of Requirements R1 and R2 to guard against the risk of unauthorized deletion or modification. Pursuant to section 215(d)(2) of the FPA,[9] the Commission proposes to approve proposed Reliability Standard CIP-015-1.

However, proposed Reliability Standard CIP-015-1 is not fully responsive to the Commission's directive to implement INSM for the "CIP-networked environment." In particular, the proposed Standard may not adequately defend against attacks that circumvent network perimeter-based security controls. Attacks external to the electronic security perimeter may compromise systems, such as electronic access control or

7 Order No. 887, 182 FERC ¶ 61,021 at P 3.
8 *Id.* P 2.
9 16 U.S.C. 824o(d)(2).

monitoring systems (EACMS)[10] and physical access control systems (PACS),[11] and then infiltrate the perimeter as a trusted communication, thus limiting the effectiveness of an approach that employs INSM only within the electronic security perimeter. Accordingly, to address this reliability and security gap, the Commission, pursuant to section 215(d)(5) of the FPA,[12] proposes to direct that NERC develop modifications to the proposed Reliability Standard CIP-015-1 to extend INSM to include EACMS and PACS outside of the electronic security perimeter.

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

On August 8, 2005, Congress enacted the EPAct 2005. The EPAct 2005 added section 215 to the FPA, which requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards,[13] including requirements for cybersecurity protection, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO subject to Commission oversight, or the Commission can independently enforce Reliability Standards.

On February 3, 2006, the Commission issued Order No. 672,[14] implementing FPA section 215. The Commission subsequently certified NERC as the ERO. The Reliability Standards developed by NERC become mandatory and enforceable after Commission

---

10 EACMS are "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." NERC, *Glossary of Terms Used in NERC Reliability Standards*, (July 22, 2024), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (NERC Glossary).

11 PACS are "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." *Id.*

12 16 U.S.C. 824o(d)(5).

13 The FPA, at 16 U.S.C. 824*o*(a)(3), defines "Reliability Standard" as a requirement, approved by the Commission, to provide for reliable operation of the bulk-power system. This definition includes cybersecurity protection, and the design of planned additions or modifications to bulk-power 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.

14

approval and apply to users, owners, and operators of the Bulk-Power System, as set forth in each Reliability Standard.[15]

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. On January 18, 2008, the Commission issued Order No. 706,[16] 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,[17] 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 BES if compromised.

The Commission is currently proposing to approve proposed Reliability Standard CIP-015-1 and proposing to direct NERC to develop modifications to the proposed Reliability Standard CIP-015-1 to extend INSM to include EACMS and PACS outside of the electronic security perimeter. The FERC-725B information collection requirements are subject to review by OMB under section 3507(d) of the Paperwork Reduction Act of 1995 (PRA).[18] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[19] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the Commission's need for this information,

---

15 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."

16 Order No. 706, 122 FERC ¶ 61,040 at P 1 (2008).

17 *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).

18 44 U.S.C. 3507(d) (2012).

19 5 CFR 1320.11 (2017).

whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques. It is part of the implementation of the Congressional mandate of the EPAct 2005 to develop mandatory and enforceable Reliability Standards to better ensure the reliability of the nation's Bulk-Power System.

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

This collection does not require industry to file the information with the Commission. However, FERC-725B does contain information collection and record retention requirements for which using current technology is an option.

The information technology to meet the information collection requirements is not specifically covered in the Reliability Standard.

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 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 a one-time and ongoing increases in reporting burden on a 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 proposed Reliability Standard, with no other increase in the cost of compliance (when compared with the current Standards). Approximately 400 of the 714 affected entities are expected to meet the Small Business Administration's definition for a small entity.[20]

20 Public utilities may fall under one of several different categories, each with a size

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, available on NERC's website.[21]

## 6. CONSEQUENCE TO FEDERAL PROGRAM IF COLLECTION WERE CONDUCTED LESS FREQUENTLY

The paperwork requirements are related to documenting compliance with substantive requirements and maintaining such documents. The frequency of the paperwork requirements was vetted and approved by industry consensus in the NERC standard development process and is ultimately meant to support the reliability of the Bulk-Power System.

## 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 ERO process to establish Reliability Standards is a collaborative process with the ERO, Regional Entities, and other stakeholders developing and reviewing drafts and providing comments.[22] The NERC-approved Reliability Standards were then submitted by NERC to the FERC for review and approval.

---

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).

21 NERC, *Rules of Procedure* (2024), https://www.nerc.com/AboutNERC/pages/rules-of-procedure.aspx.

22 Details of the ERO standards development process are available on the NERC website at http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.

The Commission published the Proposed Rule in Docket No. RM24-7-000 on September 27, 2024 (89 FR 79178).

Comments were received:

- NERC, NESCOE, OpenPolicy, and Trade Associations support the Commission's proposal to approve proposed Reliability Standard CIP-015-1
- NERC, OpenPolicy, and Trade Associations indicate that proposed Reliability Standard CIP-015-1 would improve the detection of anomalous, malicious, or unauthorized network activity
- NERC and OpenPolicy both note that improved detection of anomalous or malicious activity will strengthen responses to and recovery from threats and attacks.
- No commenters oppose approval of the proposed Reliability Standard.

OpenPolicy, while supporting approval of proposed Reliability Standard CIP-015-1, also recommends ways to strengthen the proposed Standard. For example, OpenPolicy proposes adopting scalable and modular INSM architectures to adapt to evolving cybersecurity threats by enhancing threat detection and simplifying compliance processes; and mandating robust encryption standards to secure logs against tampering and unauthorized access.

Response:
We decline to direct NERC to modify the proposed Standard to address OpenPolicy's recommendations. We note, however, that responsible entities, in addition to implementing the INSM requirements set forth in proposed Reliability Standard CIP-015-1, may voluntarily choose to adopt additional INSM practices such as those recommended by OpenPolicy. Moreover, OpenPolicy or other entities may advocate for OpenPolicy's recommendations in the NERC Reliability Standard development process.

The Final Rule published on July 2, 2025 (90 FR 28889)

**Notice of Filing and Responsive Pleadings**

As required by Section 39.5(a) of the Commission's regulations,[23] this petition presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history and complete record of development (Exhibit G), and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672 (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on May 9, 2024.

23 18 CFR 39.5.

Currently effective CIP Reliability Standards focus on preventing unauthorized access at the electronic security perimeter and do not require INSM inside trusted CIP-networked environments.[24] In Order No. 887, the Commission determined that this left a reliability gap when vendors or individuals with authorized access are deemed trustworthy but could still introduce a cybersecurity risk.[25] The Commission then concluded that requirements to implement ISNM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity will "fill a gap in the current suite of CIP Reliability Standards and improve the cybersecurity posture of the Bulk-Power System."[26] Proposed Reliability Standard CIP-015-1 requires high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to implement INSM for network traffic inside an electronic security approval. Consequently, the Commission proposes to approve proposed Reliability Standard CIP-015-1. However, the proposed Reliability Standard does not require implementation of INSM at EACMS and PACS outside of the electronic security perimeter. The proposed Standard may not adequately defend against attacks that circumvent network perimeter-based security controls. Attacks external to the electronic security perimeter may compromise systems, such as EACMS or PACS, and then infiltrate the perimeter as a trusted communication, thus limiting the effectiveness of an approach that employs INSM only within the electronic security perimeter. Consequently, the Commission is also proposing to direct NERC to develop further modifications to Reliability Standard CIP-015-1 to extend INSM to include EACMS and PACS outside of the electronic security perimeter.

## 9. **EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS**

No payments or gifts have been made to respondents.

---

24 Order No. 887, 182 FERC ¶ 61,021 at P 20.

25 *Id.* An attacker could move among devices inside a trust zone and perform actions such as: (1) escalate privileges (such as gaining administrator account privileges through a vulnerability); (2) move undetected inside the CIP-networked environment; or (3) execute a virus, ransomware or another form of unauthorized code. *Id.* P 19.

26 *Id.* P 49 (citing NERC Comments in Response to Notice of Proposed Rulemaking under Docket No. RM22-3-000 at 4-5 (current CIP Standards require "malicious communications monitoring at the Electronic Access Point on the [electronic security perimeter], not necessarily monitoring of activity of those who already have access to the network")). The Bulk-Power System is defined in the FPA as facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. 824o(a)(1).

## 10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

According to the NERC Rules of Procedure,[27] "…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

*Estimate of Annual Burden:*[28] The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the proposed revision to Reliability Standard CIP-015-1 as this is a new proposed Reliability Standard. Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems. The NERC Compliance Registry, as of July 2024, identifies approximately 1,636 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards. Of this total, we estimate that 400 entities will face an increased paperwork burden under proposed Reliability Standard CIP-015-1. Based on these assumptions, we estimate the following reporting burden:

**Annual Changes Proposed by the NOPR in Docket No.RM24-7-000**[29]

27 NERC Rules of Procedure, sec. 1502, at 91-92 (revised Nov. 28, 2023).
28 "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. 5 C.F.R. § 1320.3.
29 The paperwork burden estimate includes costs associated with the initial development

| | Number of Respondents (1) | Annual Number of Responses per Respondent (2) | Total Number of Responses (1)*(2)=(3) | Average Burden & Cost Per Response[30] (4) | Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5) | Cost per Respondent ($) (5)÷(1) |
|---|---|---|---|---|---|---|
| Create one or more documented process(es) (R1) | 400 | 1 | 400 | 40 hrs.; $3,880 | 16,000 hrs.; $1,552,000 | $3,880 |
| Create documentation detailing network data feed(s) and reason (R1.1) | 400 | 1 | 400 | 60 hrs.; $5,820 | 24,000 hrs.; $2,328,000 | $5,820 |
| Create documentation of: anomalous events and baseline used to detect anomalous | 400 | 1 | 400 | 60 hrs.; $5,820 | 24,000 hrs.; $2,328,000 | $5,820 |

of a policy to address the requirements.

30 This burden applies in Year One to Year Three.

The hourly cost for wages is based in part on the average of the occupational categories from the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm) plus benefits:

Legal (Occupation Code: 23-0000): $162.66
Electrical Engineer (Occupation Code: 17-2071): $79.31
Office and Administrative Support (Occupation Code: 43-0000): $48.59
($162.66 + $79.31 + $48.59) ÷ 3 = $96.85
The figure is rounded to $97.00 for use in calculating wage figures in this NOPR.

| | | | | | | |
|---|---|---|---|---|---|---|
| events (R1.2) | | | | | | |
| Create documentation of methods to: evaluate anomalous activity; response to detected activity; and escalation process(es) (R1.3) | 400 | 1 | 400 | 60 hrs.; $5,820 | 24,000 hrs.; $2,328,000 | $5,820 |
| Create documentation of: data retention process(es); system configuration(s), or system-generated report(s) (R2) | 400 | 1 | 400 | 60 hrs.; $5,820 | 24,000 hrs.; $2,328,000 | $5,820 |
| Create documentation of how the collected data is being protected (R3) | 400 | 1 | 400 | 60 hrs.; $5,820 | 24,000 hrs.; $2,328,000 | $5,820 |
| Total burden for FERC-725B under CIP-015-1 | | | 2,400 | | 136,000 hrs.; $13,192,000 | $32,980 |

The responses and burden hours for Years 1-3 will total respectively as follows:

- Year 1-3 each: 2,400 responses; 136,000 hours
- The annual cost burden for each year One to Three is $13,192,000.

## 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 due to the 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 Commission would incur costs associated with processing filings under the final rule, and in obtaining OMB clearance under the PRA. The estimated processing cost total $207,787 annually. The Commission estimates receiving 20 informational filings per year under the final rule, with each filing estimated to take approximately 100 hours to analyze and process, totaling the number of hours and cost of one FTE.

The estimated PRA Administrative Cost of $8,396 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.

As shown in the table below, $ is the sum of the estimated annual federal cost of analyzing and processing the filings (which is the annual salary for one Full-Time Equivalent (FTE) of $207,786) plus the estimated PRA administrative cost of $8,396.

**Table 14**
**Estimated Annual Federal Costs**

| FERC-725B | Number of Employees (FTEs) | Estimated Annual Federal Cost |
|---|---|---|

| | | |
|---|---|---|
| Analysis and Processing of Filings | 1 | $207,786 |
| Paperwork Reduction Act Administrative Cost | | $8,396 |
| **TOTAL** | | $216,182 |

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

CIP-015-1 Presents new burden of 2,400 responses and 136,000 hrs. as stated above in the table within section #12.

## 16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

There is no tabulating, statistical or publication plans in accordance with the final rule.

## 17. DISPLAY OF THE EXPIRATION DATE

The expiration date is displayed in a table posted on ferc.gov at https://www.ferc.gov/information-collections.

## 18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.