

Supporting Statement for:

FERC-725B, Revisions in Critical Infrastructure Protection Reliability Standards for RD25-8 (for CIP-002-8) and Renewal for CIP Standards update of CIP-002-8, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1, CIP-013-3, CIP-014-3, and CIP-015-1.

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 (CIP Reliability Standards) and renew the collection for an additional three years.

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, Congress enacted the Energy Policy Act of 2005.¹ The Energy Policy Act of 2005 added a new section 215 to the FPA,² which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards,³ 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. 672,⁴ 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

¹ Energy Policy Act of 2005, Pub. L. No. 109-58, sec. 1261 *et seq.*, 119 Stat. 594 (2005).

² 16 U.S.C. 824o.

³ 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).

⁴ *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).

Bulk-Power System, as set forth in each Reliability Standard.⁵ The CIP Reliability Standards require entities to comply with specific requirements to safeguard critical cyber assets. These standards are result-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. 706,⁶ 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. 791,⁷ 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)⁸ 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 Systems⁹ are categorized as low impact systems. Most requirements in the CIP

⁵ 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.”

⁶ Order No. 706, 122 FERC ¶ 61,040 at P 1.

⁷ *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).

⁸ 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).

⁹ 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

Reliability Standards apply to high and medium impact systems; however, a technical controls requirement in Reliability standard 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.¹⁰

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

On March 19, 2026, the order within RD25-8 approved Reliability Standard CIP-002-8 related to the identification and categorization of BES cyber systems and their associated BES cyber assets. The Commission approved the proposed Reliability Standard CIP-002-8 pursuant to section 215(d)(2) of the FPA because the Standard would advance reliability by revising the threshold for applicable transmission owners and transmission operators to categorize their BES cyber systems based on the impact to their associated facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable would affect the reliability of the BES. Also, to revise the definition of the term control center in the NERC Glossary to alleviate confusion from a lack of common understanding of the term “control” as opposed to “authority”.

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.

¹⁰ 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).

The CIP Reliability Standards currently consist of 14 standards specifying a set of requirements that entities must follow to ensure the cyber and physical security of the Bulk-Power System. There is also one physical security standard.

- CIP-002-8 (formerly CIP-002-7) a 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-003-10 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-004-8 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-005-8 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-006-7.1 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-007-7.1 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-008-7.1 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-009-7.1 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-010-5 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-011-4.1 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-012-2 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-013-3 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.
- CIP-014-3 Physical Security: Set out 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.
- CIP-015-1 Internal Network Security Monitoring: purpose is to improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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.¹¹ The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.¹²

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

¹¹ Order No. 822, 154 FERC ¶ 61,037 at 32.

¹² Order No. 706, 122 FERC ¶ 61,040 at 72.

requirements for which using current technology is an option.

The use of current or improved technology is not covered in Reliability Standards and is therefore left to the discretion of each reporting entity. Commission staff estimates that nearly all of the respondents are likely to make and keep related records in an electronic format. Each of the eight Regional Entities has a well-established compliance portal for registered entities to electronically submit compliance information and reports. 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.

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 Generator Operators, Generator Owners,) due to the changes in the Reliability Standard, with no other increase in the cost of compliance (when compared with the current Standards). Approximately 288 of the affected entities are expected to meet the Small Business Administration's definition for a small entity.¹³

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 sections 507 and 508, available on NERC's website.¹⁴

¹³ 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).

¹⁴ See generally NERC, *Rules of Procedure* (2024),

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 of the eleven modified CIP Reliability Standards. 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.

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 ERO process to establish Reliability Standards is a collaborative process with the ERO, Regional Entities, and other industry stakeholders developing and reviewing drafts and providing comments.¹⁵ The NERC-approved Reliability Standards were then submitted by NERC to the Commission for review and approval.

The Commission published the Proposed Rule in Docket No. RM24-8-000 on September 23, 2026 (90 FR 45685). Comments on the proposed rule were due by November 24, 2025. The Final Rule Published on March 24, 2026 (91 FR 13957). The renewal notices were published 60-day notice¹⁶ and 30-day¹⁷ notice were published with no comments received.

<https://www.nerc.com/AboutNERC/pages/rules-of-procedure.aspx>.

¹⁵ 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.

¹⁶ February 17, 2026 (91 FR 7274)

¹⁷ April 27, 2026 (91 FR 22530)

The Commission Order update for CIP-002-8 was issued on March 19, 2026, and published on March 24, 2026 (91 FR 14013), for RD25-8. The combined notice with a re-publication of the renewal with RD25-8 published for the 30-day notice on June 12, 2026 (91 FR 35681).

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

According to the NERC Rules of Procedure,¹⁸ "...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

The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the revisions to Reliability Standards filed by NERC for Commission approval. Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.

¹⁸ NERC Rules of Procedure, sec. 1502, at 91-92 (revised Nov. 28, 2023).

*Estimate of Annual Burden:*¹⁹ As of June 2025, the NERC Compliance Registry identifies approximately 1,673 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards. Based on these assumptions, the estimated reporting burden is as follows:

FERC-725B - (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards) for IC26-16-000 (Renewal)					
	Number and Type of Respondent²⁰ (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1) *(2) = (3)	Average Burden per Response (Hours) & Cost per Response (4)	Total Annual Burden (Hours) & Total Annual Cost²¹ (3) *(4) = (5)
CIP-002-8 (Carried over from table below for RD25-8)	1,573	1	1,573	2 hrs.; \$194	3,146 hrs.; \$305,162
	100	1	100	4 hrs.; \$388	400 hrs.; \$38,800
CIP-003-10	1,579	156.15	246,561	1.56 hrs.; \$120.59	384,635 hrs.; \$29,732,285.50

19 “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.

20 The number of respondents is based on the NERC Compliance Registry as of June 22, 2025. Currently there are 1,508 unique NERC Registered, subtracting 16 Canadians Entities yields 1492 U.S. entities.

21 The estimates for cost per hour are \$77.30/hour (averaged based on the following occupations):

- Manager (Occupational Code: 11-0000): \$83.41/hour; and
- Electrical Engineer (Occupational Code 17-2071): \$71.19/hour. The estimated hourly cost (salary plus benefits) is a combination of the following categories from the Bureau of Labor Statistics (BLS) website, May 2025
http://www.bls.gov/oes/current/naics2_22.htm.

CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1, CIP-009-7.1, CIP-010-5, CIP-011-4.1	100	4	400 (total per standard)	600 hrs.; \$46,380	240,000 hrs., \$18,552,000 (total for all standards)
CIP-013-3	400	1	400	30 hrs.; \$2,319	12,000 hrs.; \$927,600
CIP-014-3	321	1	321	2 hrs.; \$154.6	642 hrs.; \$49,626.60
CIP-012-2	724	1	724	83 hrs.; \$6,415.90	60,092 hrs.; \$4,645,111.60
CIP-15-1	400	6	2,400	56.67 hrs. \$4,380.59	136,008 hrs.; \$10,513,418.40
Total Burden One time burden for years 1-3 from recently approved RM24-8 affecting the following CIP Standards: CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7.1, CIP-007-7.1, CIP-008-7.1,	4000 (400 per standard)	1	4000 (400 per standard)	577 (57.7 per standard)	230,800 (23,080 per standard)

CIP-009-7.1, CIP-010-5, CIP-011-4.1, and CIP-013-3					
18 CFR 35.48(b) Voluntary filing seeking incentive rate treatment for cybersecurity investment	50	1	50	80 hrs.; \$6,184	4,000 hrs.; \$309,200
18 CFR 35.48(h) Annual informational filing	50	1	50	40 hrs.; \$3,092	2,000 hrs.; \$154,600
Total Burden of FERC-725B Renewal			259,370		1,073,723 hrs.; \$82,998,787.90

RD25-8 (Changes):

The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the proposed revisions to Reliability Standard CIP-002-8. Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems. The NERC Compliance Registry, as of June 2025, identifies approximately 1,673²² U.S. entities that are subject to mandatory compliance with Reliability Standards.

Of this total, we estimate that 1,573 entities will face a minor increase in paperwork burden of two hours each for a total burden hours increase of 3,146 at \$97²³ per hour for

²² The “Number of Entity” data is compiled from the June 2025 edition of the NERC Compliance Registry.

²³ The hourly cost for wages is based in part on the average of the occupational

\$194 per entity and a total \$305,162 burden for the first year and ongoing burdens in addition to the burden already accounted for in the OMB control number for CIP Reliability Standards.

Additionally, we estimate that another 100 entities will have a burden of four hours each for a total burden hour increase of 400 at \$97 per hour for a total burden of \$38,800 for the first year and ongoing burdens in addition to the burden already accounted for in the OMB control number for CIP Reliability Standards.

Changes for CIP-002-8 in FERC-725B - (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards)					
	Number and Type of Respondent²⁴ (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1) *(2) = (3)	Average Burden per Response (Hours) & Cost per Response (4)	Total One-time Burden (Hours) & Total Annual Cost²⁵ (\$) (3) *(4) = (5)
CIP-002-8	1,573	1	1,573	2 hrs.; \$194	3,146 hrs.; \$305,162

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 \div 3 = \96.85). The figure is rounded to \$97.00 for use in calculating wage figures in this Order.

²⁴ The number of respondents is based on the NERC Compliance Registry as of June 22, 2025. Currently there are 1,508 unique NERC Registered, subtracting 16 Canadians Entities yields 1492 U.S. entities.

²⁵ The estimates for cost per hour are \$77.30/hour (averaged based on the following occupations):

- Manager (Occupational Code: 11-0000): \$83.41/hour; and
- Electrical Engineer (Occupational Code 17-2071): \$71.19/hour. The estimated hourly cost (salary plus benefits) is a combination of the following categories from the Bureau of Labor Statistics (BLS) website, May 2025
http://www.bls.gov/oes/current/naics2_22.htm.

	100	1	100	4 hrs.; \$388	400 hrs.; \$38,800
Total for one time burden for CIP-002-8	1,673		1,673		3,546 hrs.; \$343,962

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 \$213,003 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 \$8,404 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, \$221,407 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 \$213,003) plus the estimated PRA administrative cost of \$8,404.

Table 14
Estimated Annual Federal Costs

FERC-725B	Number of Employees (FTEs)	Estimated Annual Federal Cost
Analysis and Processing of Filings	1	\$213,003
Paperwork Reduction Act Administrative Cost		\$8,404
TOTAL		\$221,407

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

The updated CIP standards present new burden changes of 400 responses and 23,800 hrs. from RM24-8 already approved as well as the RD25-8 burden of 1,673 respondents for CIP-002-8 as stated above in the table within section #12. Making a total of 4,000 responses and 230,800 burden hrs. The Change due to Adjustment represents the updated burden for CIP 2-8 which has just an update in burden due to normal fluctuation, updated from 1,579 to 1,673 respondents. Also removing unnecessary double report burden and CIP-012-2 one time burden reported for RD24-3 was removed for this renewal.

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	259,370	262,733	0	-3354
Annual Time Burden (Hrs.)	1,073,723	2,639,597	0	-1,565,874
Annual Cost Burden (\$)	\$0	\$0	\$0	\$0

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

There is no tabulating, statistical or publication plans in accordance with 725B.

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>.

FERC-725B (OMB Control No. 1902-0248)
Renewal: IC26-16-000
RD25-8 for CIP-002-8 update Issued March 19, 2026

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.