

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. RD24-3-000]

COMMISSION INFORMATION COLLECTION ACTIVITIES (FERC-725B);
COMMENT REQUEST; EXTENSION

(May 23, 2024)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of information collection and request for comments.

SUMMARY: In compliance with the requirements of the Paperwork Reduction Act of 1995, the Federal Energy Regulatory Commission (Commission or FERC) is soliciting public comment on the currently approved information collection, FERC-725B, Mandatory Reliability Standards, Critical Infrastructure Protection (CIP) (Update for CIP-012-1 to version CIP-012-02) Cyber Security – Communications between Control Centers.

DATES: Comments on the collection of information are due [**INSERT DATE 60 days after date of publication in the Federal Register**].

ADDRESSES: You may submit copies of your comments (identified by Docket No. RD24-3-000) by one of the following methods:

Electronic filing through <https://www.ferc.gov>, is preferred.

- Electronic Filing: Documents must be filed in acceptable native applications and print-to-PDF, not in scanned or picture format.
- For those unable to file electronically, comments may be filed by USPS mail or by other delivery methods:

- o Mail via U.S. Postal Service Only: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, DC 20426.
- o All other delivery services: Federal Energy Regulatory Commission, Office of the Secretary, 12225 Wilkins Avenue, Rockville, MD 20852.

Instructions: All submissions must be formatted and filed in accordance with submission guidelines at: <https://www.ferc.gov>. For user assistance, contact FERC Online Support by e-mail at ferconlinesupport@ferc.gov, or by phone at (866) 208-3676 (toll-free).

Docket: Users interested in receiving automatic notification of activity in this docket or in viewing/downloading comments and issuances in this docket may do so at <https://www.ferc.gov>.

FOR FURTHER INFORMATION: Jean Sonneman may be reached by e-mail at DataClearance@FERC.gov, telephone at (202) 502-6362.

SUPPLEMENTARY INFORMATION:

Title: FERC-725B, Mandatory Reliability Standards, Critical Infrastructure Protection (CIP) (Update to CIP-012-2)

OMB Control No.: 1902-0248

Type of Request: Revision of a currently approved FERC-725B information collection requirements with changes to the reporting requirements.

Abstract: 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 Federal Power Act (FPA),²

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.

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 the North American Electric Reliability Corporation (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.⁵ The CIP Reliability Standards require entities to comply with

³ Section 215 of the FPA 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.

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).

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

specific requirements to safeguard bulk electric system (BES) Cyber Systems⁶ and their associated BES 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.

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. 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 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

responsible for performing various specified reliability functions. We collectively refer to these as “entities.”

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), [Glossary of Terms.pdf \(nerc.com\)](#). 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.

Reliability standard CIP-012, described below, applies to all (low, medium and high) impact Control Centers.

The FERC-725B information collection requirements are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.⁷ OMB's regulations require approval of certain information collection requirements imposed by agency rules.⁸ 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, 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.

Reliability Standard CIP-012-2 – Communications between Control Centers: requires entities to protect the confidentiality, integrity, and availability and integrity of data transmitted between Control Centers that could lead to mis-operation or instability on the Bulk-Power System. Specifically, the Reliability Standard CIP-012-2 is revised to add requirements for entities to provide protections of the availability of communication links and sensitive data transmitted between BES Control Centers. It is part of the

⁷ 44 U.S.C. 3507(d) (2012).

⁸ 5 CFR 1320.11 (2017).

implementation of the Congressional mandate of the Energy Policy Act of 2005 to develop mandatory and enforceable Reliability Standards to better ensure the reliability of the nation’s Bulk-Power System.

Type of Respondents: Business or other for profit, and not for profit institutions.

*Estimate of Annual Burden:*⁹ The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the proposed revision to CIP Reliability Standard CIP-012-2 as compared to the current Commission-approved Reliability Standard CIP-012-1. As discussed above, the immediate order addresses the area of modification to the CIP Reliability Standards: modifications to provide protections of the availability of communication links and sensitive data transmitted between BES Control Centers.

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.¹⁰ The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.¹¹ The NERC Compliance Registry, as of March 15, 2024, identifies approximately 1,610 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards. Of this total, we estimate that 730

⁹ “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.

¹⁰ Order No. 822, 154 FERC ¶ 61,037 at 32.

¹¹ *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, at P 72 (2008); order on reh’g, Order No. 706-A, 123 FERC ¶ 61,174 (2008); order on clarification, Order No. 706-B, 126 FERC ¶ 61,229 (2009).

entities will face an increased paperwork burden under proposed Reliability Standard CIP-012-2. Based on these assumptions, we estimate the following reporting burdens:

FERC-725B, Modifications in Docket No. RD24-3-000					
	No. of Respondents (1)	No. of Responses¹² per Respondent (2)	Total No. of Responses (1)X(2)=(3)	Avg. Burden Hrs. & Cost Per Response¹³ (4)	Total Annual Burden Hours & Total Annual Cost (3)X(4)=5
Implementation of Documented Plan(s) (Requirement R1) ¹⁴	730	1	730	42 hrs.; \$4,493.16	30,660 hrs.; \$3,280,006.80

¹² We consider the filing of an application to be a “response.”

¹³ The hourly cost for wages plus benefits is based on the average of the occupational categories for 2024 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Information Security Analysts (Occupation Code: 15-1212): \$80.62

Computer and Mathematical (Occupation Code: 15-0000): \$74.16

Legal (Occupation Code: 23-0000): \$160.24

Computer and Information Systems Managers (Occupation Code: 11-3021): \$112.88

These various occupational categories’ wage figures are averaged as follows: $\$80.62/\text{hour} + \$74.16/\text{hour} + \$160.24/\text{hour} + \$112.88/\text{hour} \div 4 = \$106.975/\text{hour}$ (\$106.98 rounded). The resulting wage figure is rounded to \$106.98/hour for use in calculating wage figures in the Final Rule in Docket No. RD24-3-000.

¹⁴ This includes the record retention costs for the one-time and the on-going reporting documents.

Document Identification of methods to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification (Requirement R1.1) ¹⁴	730		1	730	20 hrs.; \$2,139.60	14,600 hrs.; \$1,561,908
Document Identification of methods to mitigate the risk(s) posed by loss of the ability to communicate (Requirement R1.2) ¹⁴	730		1	730	60 hrs.; \$6,418.80	43,800 hrs.; \$4,685,724
Document Identification of methods to use to initiate the recovery of communication links (Requirement R1.3) ¹⁴	730		1	730	100 hrs.; \$10,698	73,000 hrs.; \$7,809,540
Document Identification of where the implemented method(s) as required in Parts 1.1 and 1.2 (Requirement R1.4) ¹²	730		1	730	50 hrs.; \$5,349	36,500 hrs.; \$3,904,770

Document identification of the responsibilities of each Responsible Entity (if <u>not</u> owned by same Responsible Entity) required in Parts 1.1, 1.2 and 1.3 (Requirement R1.5) ¹⁴	730	1	730	50 hrs.; \$5,349	36,500 hrs.; \$3,904,770
Maintaining Compliance (ongoing, starting in Year 2)	730	1	730	1 hr.; \$106.98	730 hrs.; \$78,095.40
Total (one-time, in Year 1)			4,380		235,060 hrs.; \$25,146,718.80
Total (ongoing, starting in Year 2)			730		730 hrs.; \$78,095.40

1. The one-time burden (in Year 1) for the FERC-725B information collection will be averaged over three years:
 - $235,060 \text{ hours} \div 3 = 78,353$ (rounded) hours/year over Years 1-3
 - The number of one-time responses for the FERC-725B information collection is also averaged over Years 1-3: $4,380 \text{ responses} \div 3 = 1,460$ responses/year
2. The average annual number (for Years 1-3) of responses and burden for one-time and ongoing burden will total:

- 2,190 responses [1,460 responses (one-time) + 730 responses (ongoing)]
- 79,083 burden hours [78,353 hours (one-time) + 730 hours (ongoing)] *Comments:*
Comments are invited on: (1) whether the collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (2) the accuracy of the agency's estimate of the burden and cost of the collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility and clarity of the information collection; and (4) ways to minimize the burden of the collection of information on those who are to respond, including the use of automated collection techniques or other forms of information technology.

Debbie-Anne A. Reese,
Acting Secretary.