E 6717-01-P

DEPARTMENT OF ENERGY
Federal Energy Regulatory Commission
[Docket No. RD23-3-000]
Commission Information Collection Activities (FERC-725B(5)); Comment Request; Extension

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(5), (Mandatory Reliability Standards, Critical Infrastructure Protection (CIP-003-9)-Temporary Placeholder for FERC-725B that is pending approval at OMB.

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. RD23-3-000) by one of the following methods:

Electronic filing through http://www.ferc.gov, is preferred.

- Electronic Filing: Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format.
- For those unable to file electronically, comments may be filed by USPS mail or by hand (including courier) delivery:
    - Mail via U.S. Postal Service Only: Addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, DC 20426.
    - Hand (including courier) delivery: Deliver to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

Instructions: All submissions must be formatted and filed in accordance with submission guidelines at: http://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 http://www.ferc.gov.

FOR FURTHER INFORMATION CONTACT: Ellen Brown may be reached by e-mail at DataClearance@FERC.gov, telephone at (202) 502-8663.

SUPPLEMENTARY INFORMATION:

Title: FERC-725B(5) (Mandatory Reliability Standards, Critical Infrastructure Protection (CIP-003-9)) - Temporary Placeholder for FERC-725B that is pending approval at OMB

OMB Control No.: 1902-NEW

Type of Request: New collection request for FERC-725B(5) - temporary placeholder for 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] which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards,[3] including requirements for

---

[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] 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. *Id.* at 824o(a)(3).

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 specific requirements to safeguard bulk electric system (BES) Cyber Systems[6] and their

---

[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 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), 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

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 Reliability standard CIP-003, described below, applies only to low impact systems.

The Commission is currently revising CIP-003 on this submission of Docket No. RD23-3-000 to update CIP-003-8 to CIP-003-9. 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

---

> 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.

[7] 44 U.S.C. 3507(d) (2012).

[8] 5 CFR 1320.11 (2017).

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-003-9 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 on the Bulk-Power System. Specifically, the Reliability Standard CIP-003-9 is revised to add requirements for entities to adopt mandatory security controls for vendor electronic remote access used at low impact BES Cyber Systems. It is part of the 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-003-9 as compared to the current Commission-approved Reliability Standard CIP-003-8. As discussed above, the immediate order addresses the area of modification to the CIP Reliability Standards: adopting mandatory security controls for vendor electronic remote access used at low impact BES Cyber Systems.

---

[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 Title 5 Code of Federal Regulations 1320.3.

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 January 4, 2023, identifies approximately 1,592 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,579 entities will face an increased paperwork burden under Reliability Standard CIP 003-9, estimating that a majority of these entities will have one or more low impact BES Cyber Systems. Based on these assumptions, the Commission estimates the total annual burden and cost as follows:

RD23-3-000 Commission Order (Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards CIP-003-9)						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response [12] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**

[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).

[12] The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for 2022 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Legal (Occupation Code: 23-0000): $145.35

Electrical Engineer (Occupation Code: 17-2071): $77.02

Office and Administrative Support (Occupation Code: 43-0000): $43.62

($145.35 + $77.02 + $43.62) ÷ 3 = $88.66. The figure is rounded to $89.00 for use in calculating wage figures in this Commission Order.

Create vendor remote access policy (one-time)[13]	1,579	1	1,579	60 hrs. $5,340	94,740 hrs. $8,431,860	$5,340
Updates and reviews of vendor remote access policy (ongoing)	1,579	1	1,579	3.5 hrs. $311.50	5,527 hrs. (rounded) $491,903	$311.50
Total burden for FERC-725B(5) under CIP-003-9			3,158		100,267 hrs. $8,923,763	

The one-time burden of 94,740 hours that only applies for Year 1 will be averaged over three years (94,740 hours ÷ 3 = 31,580 hours/year over three years). The number of responses is also averaged over three years (1,579 responses ÷ 3 = 526.33 responses/year).

The ongoing burden of 5,527 hours/year applies for only Years 2 and beyond (5,527 hours (Year 2) + 5,527 hours (Year 3) ÷ 3 = 5,527 hours. Similarly, the number of responses is also averaged over three years ((1,579 responses (Year 2) + 1,579 (Year 3)) ÷ 3 = 1,579[14]).

[13] This one-time burden applies in Year One only.

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

Year 1: 526.33 responses; 31,580 hours

Year 2: 526.33 responses; 31,580 hours

Year 3: 526.33 responses; 31,580 hours

The responses and burden hours for Years 1-3 will total respectively as follows for Ongoing and beyond: 1,579 responses and 5,527 hours

The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: $8,431,860 (Onetime)
- Years 2 and 3: $491,903 (Ongoing)

The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to policy development, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

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.

Dated: March 24, 2023.

Debbie-Anne A. Reese,
Deputy Secretary.

[FR Doc. 2023-06600 Filed: 3/29/2023 8:45 am; Publication Date: 3/30/2023]