UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. IC21-26-000]

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

(June 30, 2021)

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).

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. IC21-26-000) 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: Ellen Brown may be reached by e-mail at DataClearance@FERC.gov, telephone at (202) 502-8663.

SUPPLEMENTARY INFORMATION:

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

OMB Control No.: 1902-0248

Type of Request: Three-year extension of the FERC-725B information collection requirements with no 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 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 Bulk-Power System, as set forth in each Reliability Standard.[5] The CIP Reliability

---

[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).

[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*

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,[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.

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

Medium impact systems include smaller control centers, ultra-high voltage transmission, and large substations and generating facilities. The remainder of the BES Cyber Systems[9] 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. 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]

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 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 12 standards specifying a set of requirements that entities must follow to ensure the cyber and physical security of the Bulk-Power System. There are 12 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 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-008-6 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-009-6 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.

- 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:[11] 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.[12] The CIP

[11] CIP-012-1: Communications between Control Centers will be subject to enforcement by July 1, 2022.

[12] Order No. 822, 154 FERC ¶ 61,037 at 32.

Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.[13]

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).					
	Number and Type of Respondent[14] (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden per Response (Hours) [15]& Cost per Response (4)**	**Total Annual Burden (Hours) & Total Annual Cost[16] ($) (3)*(4)=(5)**
CIP-003-8[17]	1,149[18]	300	344,700	1.5 hrs.; $127.53	517,050 hrs; $43,959,591
CIP-003-8[19]	1,149	1	1,149	20 hrs.; $1,700.40	23,220 hrs.; $1,974,164.4

[13] Order No. 706, 122 FERC ¶ 61,040 at 72.

[14] The number of respondents is based on the NERC Compliance Registry as of June 22, 2021. Currently there are 1,508 unique NERC Registered, subtracting 16 Canadians Entities yields 1492 U.S. entities.

[15] Of the average estimated 295.702 hours per response, 210 hours are for recordkeeping, and 85.702 hours are for reporting.

[16] The estimates for cost per hour are $85.02/hour (averaged based on the following occupations):

- Manager (Occupational Code: 11-0000): $97.89/hour; and
- Electrical Engineer (Occupational Code 17-2071): $72.15/hour, from the Bureau of Labor and Statistics at http://bls.gov/oes/current/naics3_221000.htm, as of June 2021.

[17] Updates and reviews of low impact TCA assets (ongoing)

[18] We estimate that 1,161 entities will face an increased paperwork burden under Reliability Standard CIP 003-8, estimating that a majority of these entities will have one or more low impact BES Cyber Systems.

[19] Update paperwork for access control implementation in Section 2 and Section 3 (ongoing)

CIP-003-8[20]	343	1	343	1 hr.; $85.02	343 hrs.; $29,161.86
CIP-002-5.1, CIP-004-6, CIP-005-7, CIP-006-6, CIP-007-6, CIP-008-6, CIP-009-6, CIP-010-3, CIP-011-2	343	1	343	600[21] hrs.; $51,012	205,800 hrs., $17,497,116
CIP-013-1	343	1	343	30 hrs.; $2550.60	10,290 hrs.; $874,855.80
CIP-014-2	321[22]	1	321	2 hrs.; $170.04	642 hrs.; $54,582.84
CIP-012-1	724[23]	1	724	83 hrs.; $7,056.66	60,092 hrs., $5,109,021.84
Total Burden of FERC-725B			347,923		817,437 hrs.; $69,498,493.74

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

[20] Modification and approval of cybersecurity policies for all CIP Standards

[21] 600 hr. estimate is based on ongoing burden estimate from Order No. 791, added to the 3-year audit burden split over 3 years: 600 = (640/3)+(408-(20+1)). (20+1) is the CIP-003-8 burden.

[22] 321 U.S. Transmission Owners in NERC Compliance Registry as of June 22, 2021.

[23] The number of entities and the number of hours required are based on FERC Order No. 802 which approved CIP-012-1.

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.

Kimberly D. Bose,
Secretary.