Supporting Statement for
FERC-725B (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards)

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review the revisions to the FERC-725B information collection (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards).

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 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 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

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 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.

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 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 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 THE INFORMATION IS TO BE USED AND THE CONSEQUENCES OF NOT COLLECTING THE INFORMATION

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 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 13[11] standards specifying a set of requirements that entities must follow to ensure the cyber and physical security of the Bulk-Power System.

- 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

11 Changes in FERC-725B2, when approved, will result in another 725B request to update the Reliability Standards CIP-005, CIP-010, and CIP-013.

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:[12] 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.
- CIP-014-2 Physical Security: requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations and conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process.

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.[13] The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.[14]

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

The use of current or improved technology and the medium are not covered in Reliability Standards and are therefore left to the discretion of each respondent. We think that nearly all of the respondents are likely to make and keep related records in an electronic format. 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)**

12 CIP-012-1: Communications between Control Centers will be subject to enforcement by July 1, 2022.
13 Order No. 822, 154 FERC ¶ 61,037 at 32.
14 Order No. 706, 122 FERC ¶ 61,040 at 72.

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 in order 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 one-time and ongoing increases in reporting burden on 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 revised Reliability Standards, with no other increase in the cost of compliance (when compared with the current standards). Approximately 585 of the 714 affected entities are expected to meet the SBA's definition for a small entity. [15]

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, Paragraph 2, available at NERCs website.

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

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

15 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).

The 60-day Federal Register Notice published on July 7, 2021 (86 FR 35783) and no comments were received. The 30-day notice was published on September 14, 2021 no comments are expected.

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[16], "…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

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).

16 Section 1502, Paragraph 2, available at NERCs website.

	Number and Type of Respondent[17] (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden per Response (Hours) [18]& Cost per Response (4)	Total Annual Burden (Hours) & Total Annual Cost[19] ($) (3)*(4)=(5)
CIP-002-5.1	1,492	1	1,492	20 hrs.; $1,700.40	29,840 hrs.; $2,536,996.8
CIP-003-8	1,492[20]	156.149	232,974.387	1.56 hrs.; $132.63	363,440.04 hrs.; $30,899,672.20
CIP-004-6	343	1	343	565 hrs.; $48,036.30	193,795 hrs.; $16,476,450.90
CIP-005-7	343	1	343	525 hrs.; $44,635.50	180,075 hrs.; $15,309,976.50
CIP-006-6	343	1	343	232 hrs.; $19,724.64	79,576 hrs.; $6,765,551.52
CIP-007-6	343	1	343	2,080 hrs.; $176,841.60	713,440 hrs.; $60,656,668.80

17 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.

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

19 The estimates for cost per hour are $85.02/hour (averaged based on the following

- 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.

20 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.

CIP-008-6	343	8	2744	13.225 hrs.; $1,124.39	36,288 hrs.; $3,085,205.76
CIP-009-6	343	1	343	162 hrs.; $13,773.24	55,566 hrs.; $4,724,221.32
CIP-010-3	343	1	343	1,172 hrs.; $99,643.44	401,996 hrs.; $34,177,699.92
CIP-011-2	343	1	343	86 hrs.; $7,311.72	29,498 hrs.; $2,507,919.96
CIP-012-1	724[21]	1	724	85.67 hrs.; $7,283.66	62,025.08 hrs.; $5,273,372.30
CIP-013-1	343	1	343	20 hrs.; $1,700.40	6,860 hrs.; $583,237.20
CIP-014-2	321[22]	1	321	32.71 hrs.; $2,781	10,499.91 hrs.; $888,451.35
Total Burden of FERC-725B			**240,999.387**		**2,162,899.03 hrs.; $183,889,675.53**

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 of the costs due to this 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

21 The number of entities and the number of hours required are based on FERC Order No. 802 which approved CIP-012-1.
22 321 U.S. Transmission Owners in NERC Compliance Registry as of June 22, 2021.

The Regional Entities and NERC do most of the data processing, monitoring and compliance work for Reliability Standards. Any involvement by the Commission is covered under the FERC-725 collection (OMB Control No. 1902-0225) and is not part of this request or package. The data are not submitted to FERC.

The Commission does incur the costs associated with obtaining OMB clearance under the Paperwork Reduction Act (PRA). The PRA Administrative Cost 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.

FERC-725B	Number of Employees (FTEs)	Estimated Annual Federal Cost
Analysis and Processing of Filings	0	$0
Paperwork Reduction Act Administrative Cost		$6,475
TOTAL		$6,475

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

In Order No. 822[23], the Commission directed NERC to, among other things, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers "in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." The Commission explained that Control Centers associated with responsible entities, including reliability coordinators, balancing authorities, and transmission operators, must be capable of receiving and storing a variety of bulk electric system data from their interconnected entities in order to adequately perform their reliability functions. The Commission, therefore, determined that "additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted." [24]
The Annual Number of Responses has changed due to the increase in the number of Unique NERC Registered Entities and a reduction in time per response contributed to the reduction in hours per response. Also, the removal of the one-time burden from RM17-11 and RM17-13 contributed to a large decrease of burden hours. The ongoing burden kept the burden the same overall. Any further Adjustment in estimate were due to CIP-004 through CIP-011 were separated to better represent the true estimates for each Reliability Standard instead of using a bulk number.

23 Order No. 822 is 81 FR 4177 (Jan. 26, 2016)
24 Final Rule for Critical Infrastructure Protection Reliability Standard CIP-012-1-Cyber Security-Communications Between Control Centers – published 4/13/2020 85 FR 8161

A summary of the burden added to FERC-725B information collection for CIP standards are as follows:

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	240,999	224,800	17,124	-925
Annual Time Burden (Hrs.)	2,162,899	2,119,709	119,873	-76,683
Annual Cost Burden ($)	$0	$0	$0	$0

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

There are no tabulating, statistical or publication plans.

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.