FERC-725B (OMB Control No. 1902-0248)
Final Rule (issued 1/23/2020) in Docket No. RM18-20-000
RIN: 1902-AF64
(updated 3/30/2020)

Supporting Statement for
FERC-725B (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards),
as modified by the Final Rule in Docket No. RM18-20-000

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) as implemented by the Final Rule (Order 866, issued 1/23/2020)[1] in Docket No. RM18-20-000.

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, The Electricity Modernization Act of 2005, which is Title XII of the Energy Policy Act of 2005 (EPAct 2005), was enacted into law. EPAct 2005 added a new Section 215[2] to the Federal Power Act (FPA), which requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight. In 2006, the Commission certified the North American Electric Reliability Corporation (NERC) as the ERO pursuant to FPA section 215.[3]

Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[4] the Commission approved Reliability Standard CIP-012-1 (Cyber Security – Communications between Control Centers). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted the proposed Reliability Standard for Commission approval in response to a Commission directive in Order No. 822.[5] Specifically, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to develop modifications 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)."[6]

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

1 The Order is posted in FERC's eLibrary at https://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=15449122.
2 16 U.S.C. 824o.
3 *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).
4 16 U.S.C. 824o(d)(2).
5 *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 53, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).
6 16 U.S.C. 824o(d)(5); Order No. 822, 154 FERC ¶ 61,037 at P 53.

Reliability Standard CIP-012-1 is intended to augment the currently-effective Critical Infrastructure Protection (CIP) Reliability Standards to mitigate cybersecurity risks associated with communications between bulk electric system Control Centers.[7] Specifically, Reliability Standard CIP-012-1 supports situational awareness and reliable bulk electric system operations by requiring responsible entities to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between bulk electric system Control Centers.[8] Accordingly, the Commission determines that Reliability Standard CIP-012-1 is largely responsive to the Commission's directive in Order No. 822.

Reliability Standard CIP-012-1, requires a responsible entity to implement a documented plan to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers and include: a) identification of the protection used, b) identification of the security protections is applied, and c) if the Control Centers owned by different entities, identify the responsability of each party. 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.

Reporting and Recordkeeping Requirements. Reliability Standard CIP-012-1 [with the associated reporting and recordkeeping requirements highlighted in gray], excerpted from the NERC Petition, is provided at pages 9-end of this supporting statement (with highlighting added) and available in Supplementary Documents in ROCIS and reginfo.gov.

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

7 Control Center is defined as one or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary), http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers to the bulk electric system.

8 Real-time Assessment is defined in the NERC Glossary while Real-time monitoring is not.

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 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.[9]

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.

---

9 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).

8. DESCRIBE EFFORTS TO CONSULT OUTSIDE THE AGENCY: SUMMARIZE PUBLIC COMMENTS AND THE AGENCY'S RESPONSE TO THESE COMMENTS

Each FERC rulemaking (both proposed and final rules) is published in the Federal Register thereby providing public utilities and licensees, state commissions, Federal agencies, and other interested parties an opportunity to submit data, views, comments or suggestions concerning the proposed collections of data.

The NOPR was published[10] in the Federal Register on 4/24/2019. No public comments on issues related to the Paperwork Reduction Act were submitted in response to the NOPR.

The Final Rule was published in the Federal Register on 2/7/2020 (85 FR 7197).

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[11], "…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

NERC's Reliability Standard CIP-012-1 results in one-time and ongoing increases to burden in the reporting requirements imposed on Reliability Coordinators, Generator Operators, Generator

10 84 FR 17105
11 Section 1502, Paragraph 2, available at NERCs website

Owners, Interchange Coordinators/Authorities, Transmission Operators, Balancing Authorities, and Transmission Owners.

The NERC Compliance Registry, as of December 2019, identifies approximately 1,482 unique U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 719 entities will face an increased paperwork burden under Reliability Standard CIP-012-1. Based on these assumptions, we estimate the following reporting burden:

FERC-725B, Modifications Due to the Final Rule in Docket No. RM18-20-000					
	No. of Respondents (1)	**No. of Responses[12] per Respondent (2)**	**Total No. of Responses (1)X(2)=(3)**	**Avg. Burden Hrs. & Cost Per Response[13] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)X(4)=5**
Implementation of Documented Plan(s) (Requirement R1)[14]	719	1	719	128 hrs.; $11,776	92,032 hrs.; $8,466,944
Document Identification of Security Protection (Requirement R1.1) [14]	719	1	719	40 hrs.; $3,680	28,760 hrs.[15]; $2,645,920
Identification of Security Protection Application (if owned by same Responsible Entity) (Requirement R1.2) [14]	719	1	719	20 hrs.; $1,840	14,380 hrs.[16]; $1,322,960
Identification of Security Protection Application (if not owned by same Responsible Entity) (Requirement R1.3) [14]	719	1	719	160 hrs.; $14,720	115,040 hrs.[17]; $10,583,680
Maintaining Compliance				83 hrs.;	59,677 hrs.;

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 2018 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Information Security Analysts (Occupation Code: 15-1122): $61.49
Computer and Mathematical (Occupation Code: 15-0000): $63.54
Legal (Occupation Code: 23-0000): $142.86
Computer and Information Systems Managers (Occupation Code: 11-3021): $98.81.

These various occupational categories' wage figures are averaged as follows: $61.49/hour + $63.54/hour + $142.86/hour + $98.81/hour) ÷ 4 = $91.70/hour. The resulting wage figure is rounded to $92.00/hour for use in calculating wage figures in the Final Rule in Docket No. RM18-20-000.

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

15 The Final Rule inadvertently says "28,560 hrs.," but that figure is corrected here.

16 The Final Rule inadvertently says "14,280 hrs.," but that figure is corrected here.

17 The Final Rule inadvertently says "14,240 hrs.," but that figure is corrected here.

In Year 1, we estimate 2,876 responses and 250,212 burden hours (one-time). For Year 2 and Year 3, we estimate 719 responses and 59,677 burden hours (ongoing) each. Averaging the responses and burden hours over Years 1-3, we get estimated annual averages of:

- 1,438 responses [(2,876+719+719)/3] per year
- 123,188.67 burden hours [(250,212+59,677+59,677)/3] per year.

These average annual figures over Years 1-3 will be used in ROCIS and reginfo.gov.

The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) developing the documented plans to protect the communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers; (2) developing and documenting the identification of security protection ; (3 developing and documenting maintaining compliance. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to plan and procedure development, while costs in years 2 and 3 will reflect the burden associated with maintaining the protection of the communications links and sensitive bulk electric system data .

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

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	Estimated Annual Federal

	(FTEs)	Cost
Analysis and Processing of Filings	0	$0
Paperwork Reduction Act Administrative Cost		$4,832
TOTAL		$4,832

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

In Order No. 822, 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."

NERC posits that the proposed Reliability Standard CIP-012-1 "requires Responsible Entities to develop and implement a plan to address the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity) of Real-time Assessment and Real-time monitoring data while being transmitted between applicable Control Centers." The required plan must include the following: (1) identification of security protections; (2) identification of where the protections are applied; and (3) identification of the responsibilities of each entity in case a Control Center is owned or operated by different responsible entities.

As stated in Commission Order 866, paragraph 2:

> Consistent with the directive in Commission Order No. 822, Reliability Standard CIP-012-1 improves upon the currently-effective Critical Infrastructure Protection (CIP) Reliability Standards to mitigate cyber security risks associated with communications between bulk electric system Control Centers. Specifically, Reliability Standard CIP-012-1 supports situational awareness and reliable bulk electric system operations by requiring responsible entities to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between bulk electric system Control Centers. Accordingly, the Commission approves Reliability Standard CIP-012-1 because it is largely responsive to the Commission's directive in Order No. 822 and improves the cyber security posture of responsible entities. We also approve the associated violation risk factors and violation severity levels, implementation plan, and effective date.

A summary of the burden added to FERC-725B information collection due to the Final Rule in RM18-20-000 follows:

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	224,800	223,362	0	1,438
Annual Time Burden (Hrs.)	2,119,709	1,996,520	0	123,189
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 http://www.ferc.gov/docs-filing/info-collections.asp.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.

The standard [highlighting added] as proposed by NERC in its Petition

CIP-012-1 – Cyber Security – Communications between Control Centers

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

   4.2.3. A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the

generation resource or Transmission station or substation co-located with the transmitting Control Center.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC

Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.