FERC-725B2 (OMB Control No. TBD)
Notice of Proposed Rulemaking (NOPR) (issued 1/18/2018) in Docket RM17-13-000
RIN: 1902-AF48

Supporting Statement for
FERC-725B2 (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards)
as established by the NOPR in Docket RM17-13

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review and approve the FERC-725B2[1] information collection (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards) as established by the NOPR in RM17-13[2].

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[3] 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.[4]

Pursuant to section 215 of the FPA, the Commission proposes to approve Critical Infrastructure Protection (CIP) Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security --- Electronic Security Perimeters(s)), and CIP-010-3 (Cyber Security --- Configuration Change Management and Vulnerability Assessments). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 in response to directives in Order No. 829.[5] The proposed reliability standards are intended to augment the currently effective CIP Reliability Standards in order to mitigate cybersecurity risks associated with the supply chain for BES Cyber System[6].

---

1 In the NOPR in Docket RM17-13, FERC used the FERC-725B information collection (OMB Control No. 1902-0248). However, another unrelated NOPR under FERC-725B (ICR No. 201801-1902-005) is still pending review at OMB, and only one item per OMB Control No. may be pending OMB review at a time. Therefore we are usinga temporary information collection number, FERC-725B2, in order to submit this package timely to OMB. This NOPR will be submitted in FERC-725B2.

2 The NOPR (issued 1/18/2018) is available in FERC's eLibrary system at https://elibrary-backup.ferc.gov/idmws/common/OpenNat.asp?fileID=14799792.

3 16 U.S.C. 824o.

4 *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).

5 *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050, at P 43 (2016)

6 BES Cyber System is defined 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." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary) is posted at http://www.nerc.com/files/glossary_of_terms.pdf. The acronym BES refers

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

The proposed Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security --- Electronic Security Perimeters(s)), and CIP-010-3 (Cyber Security --- Configuration Change Management and Vulnerability Assessments) are to be used by NERC registered entities to mitigate cybersecurity risks associated with the supply chain for BES Cyber System The NERC Compliance Registry, as of December 2017, identifies approximately 1,250 unique U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 288 entities will face an increased paperwork burden under proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3.

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) 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/Authorities, Transmission Operators, Balancing Authorities, Transmission Owners) due to the changes in the revised Reliability Standards, with no other

to the bulk electric system.

increase in the cost of compliance (when compared with the current standards). Approximately 248 of the 288 affected entities are expected to meet the SBA's definition for a small entity.

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 these Reliability Standards will result in an unmitigated risk from software, hardware and services vulnerabilities present in the supply chain of the NERC registered entities which operate the bulk electric system.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

FERC-725B2 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

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[7] in the Federal Register on 1/25/2018.

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[8], "…a Receiving Entity shall keep in confidence and not copy, disclose, or distribute any Confidential Information or any part thereof without the

7 83 FR 3433
8 Section 1502, Paragraph 2, available at NERCs website

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 proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 will result in one-time and ongoing increases to burden in the reporting requirements imposed on Reliability Coordinators, Generator Operators, Generator Owners, Interchange Coordinators/Authorities, Transmission Operators, Balancing Authorities, and Transmission Owners.

The burden of the current versions of the standards, which are being replaced, is approved under FERC-725B. The new proposed versions of the standards in FERC-725B2 will impose a burden in addition to the existing burden. The estimated burden and cost for FERC-725B2 due to the proposed standards in the NOPR in RM17-13 follow:

FERC-725B2, as proposed in the NOPR in RM17-13-000 (Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards)						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response[9] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**

9 The loaded hourly wage figure (includes benefits) is based on the occupational categories for 2016 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Legal (Occupation Code: 23-0000): $143.68
Information Security Analysts (Occupation Code 15-1122): $66.34
Computer and Information Systems Managers (Occupation Code: 11-3021): $100.68
Management (Occupation Code: 11-0000): $81.52
Electrical Engineer (Occupation Code: 17-2071): $68.12
Management Analyst(Code: 43-0000): $63.49

These various occupational categories are weighted as follows: [($81.52)(.10) + $66.34(.315) + $68.12(.02) + $143.68(.15) + $100.68(.10) + $63.49(.315)] = $82.03. The figure is rounded to $82.00 for use in calculating wage figures in this NOPR.

Create supply chain risk management plan (one-time)[10] (CIP-013-1 R1)	288	1	288	546 hrs.; $44,772	157,248 hrs.; $12,894,336	$44,772
Updates and reviews of supply chain risk management plan (ongoing)[11] (CIP-013-1 R2)	288	1	288	30 hrs.; $2,460	8,640 hrs.; $708,480	$2,460
Develop Procedures to update remote access requirements (one time) (CIP-005-6 R1-R4)	288	1	288	50 hrs.; $4,100	14,400 hrs.; $1,180,800	$4,100
Develop procedures for software integrity and authenticity requirements (one time) (CIP-010-3 R1-R4)	288	1	288	50 hrs.; $4,100	14,400 hrs.; $1,180,800	$4,100
TOTAL (one-time, Year 1)			**864**		**186,048 hrs.; $15,255,936**	
TOTAL (ongoing, Years 2-3)			**288**		**8,640 hrs.; $708,340**	

The estimated burden is averaged over Years 1-3 in the following ways:

- The one-time burden of 186,048 hours will be averaged over three years (186,048 hours ÷ 3 = 62,016 hours/year over three years).
- The ongoing burden of 8,640 hours applies to only Years 2 and beyond. Averaged over Years 1-3 (for ROCIS submission), the annualized ongoing burden is 5,760 hours/year.
- The number of one-time responses is averaged over three years (864 responses in Year One ÷ 3 = 288 responses/year over Years 1-3).
- The number of ongoing responses is 192 (288 responses * 2 = 864 responses ÷ 3 = 192 responses) annually for Years 1-3.
- Annually, the number of responses for both one-time and ongoing responses (accounting for all averaging) is 480 responses/year.

10 One-time burdens apply in Year One only.
11 Ongoing burdens apply in Year 2 and beyond.

The responses and burden averaged for Years 1-3 will total respectively as follows:

Year 1: 480 responses; 62,016 hours
Year 2: 480 responses; 62,016 hours + 8,640 hours = 70,656 hours
Year 3: 480responses; 62,016 hours + 8,640 hours = 70,656 hours

For submission in ROCIS, the average annual response and burden hour totals for Years 1-3 are:

- Responses: 480/year
- Burden: 67,776 hours/year[12]

The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) developing the supply chain risk management plan; (2) updating the procedures related to remote access requirements; (3) developing the procedures related to software integrity and authenticity. 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 Supply Chain Risk Management (SCRM) plan and modifying it as necessary on a 15 month basis[13].

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 in the NOPR are associated with burden hours (labor) and described in Questions #12 and #15 in this supporting statement.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

Any involvement by the Commission is covered under the FERC-725 (OMB Control No. 1902-0255). The data are not submitted to FERC.

The Commission does incur the costs associated with obtaining OMB clearance for FERC-725B2 collection 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

12 (62,016 hours + 70,656 hours + 70,656 hours) ÷ 3 = 67,776 hours/year
13 The SCRM, per Reliability Standard CIP-013-1, must be updated once per 15 months. For OMB submission purposes, FERC staff is using the update frequency on an annual (i.e. 12-month) basis.

publications in the Federal Register. FERC estimates the annual cost for this effort to be $5,723.00.

FERC-725B2	Number of Employees (FTEs)	Estimated Annual Federal Cost
Analysis of Filings	0	$0
Processing of Filings	0	$0
Paperwork Reduction Act Administrative Cost		$5,723
TOTAL		$5,723

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

As the Commission previously recognized, the global supply chain provides the opportunity for significant benefits to customers, including low cost, interoperability, rapid innovation, a variety of product features and choice. However, the global supply chain also enables opportunities for adversaries to directly or indirectly affect the management or operations of companies that may result in risks to end users. Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices. We propose to determine that the supply chain risk management Reliability Standards submitted by NERC constitute substantial progress in addressing the supply chain cyber security risks identified by the Commission.

NERC registered entities that operate applicable systems listed in the Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 must develop and implement:

- one or more method(s) for determining active vendor remote access sessions;
- one or more method(s) to disable active vendor remote access;
- a method to verify the integrity of the software obtained from the software source when the method to do so is available;
- one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems which must address as applicable
    - Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity
    - Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
    - Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
    - Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

- Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System;
- Coordination of controls for:
  - vendor-initiated Interactive Remote Access;
  - system-to-system remote access with a vendor(s)
- Each Responsible Entity shall implement its supply chain cyber security risk management plan(s).

A summary of the burden added to FERC-725B2 information collection due to the NOPR in RM17-13 follows:

FERC-725B2	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	480	0	0	480
Annual Time Burden[14]	67,776	0	0	67,776
Annual Cost Burden ($)	$0	$0	$0	$0

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

There are no tabulating, statistical or tabulating analysis or publication plans for the collection of information.

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.

14 The units of measurement applied to “annual time burden” are hours.