SUPPORTING STATEMENT FOR FERC-725B, Revised Critical Infrastructure Protection Reliability Standards, as revised by NOPR in Docket RM15-14

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review the information collection requirements in the **FERC-725B, Revised Critical Infrastructure Protection Reliability Standards**.

In this NOPR (Notice of Proposed Rulemaking) in Docket RM15-14, the Commission proposes to approve seven Critical Infrastructure Protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection).

FERC-725B (OMB Control No. 1902-0248) is an existing data collection, as contained in 18 Code of Federal Regulations (CFR), Part 40.

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.[1] EPAct 2005 added a new section 215 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 by the Commission, the Reliability Standards may be enforced by the ERO, subject to Commission oversight. The North American Electric Reliability Corporation (NERC) is the Commission-certified ERO.

NERC submitted the proposed Reliability Standards in response to the Commission's Order No. 791. The proposed Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the Commission proposes to direct NERC to develop certain

[1] The Energy Policy Act of 2005, Pub. L. No 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005), codified at 16 U.S.C. 824o (2000).

modifications to Reliability Standard CIP-006-6 and to develop requirements addressing supply chain management.

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

The information collection requirements in the proposed CIP standards apply to entities registered as the following functions: balancing authorities, distribution providers, generator operators, generator owners, interchange coordinators (or interchange authorities), reliability coordinators, transmission operators, and transmission owners. Based on the NERC compliance registry, FERC estimates there are 1,363 entities in the U.S. registered for at least one of the functions listed above. Each of these entities is considered a "respondent" for the purposes of fulfilling the paperwork requirements.

The cyber security policy, process, and procedure documentation required by the CIP standards are the principal components of a cyber-security program. The main use for the information generated is to achieve and maintain a cyber-secure operational state, a process which requires vigilant monitoring of activity against documented policies and procedures. The information generated can also be used to show auditors that required cyber security policies, processes, and procedures are designed to achieve the requirement and are implemented as designed. Similarly, the applicable compliance enforcement authority (regional entity or NERC) relies upon any such documentation it is shown to measure an entity's compliance with a given requirement. The information is also used for evaluating reliability events or for enforcement actions.

If the information collection requirements did not exist then it would be difficult to monitor and enforce compliance with the standards, which could lead entities to relax their compliance with the requirements. Also, creating and maintaining documentation is integral to the task of performing cyber security, as reflected in the fact that some of the reliability standards' requirements actually require an entity to create a document (as opposed to *documenting* compliance with a requirement). Without such information collection an entity may fail to perform actions that may affect the reliability and security of the grid.

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

The use of current or improved technology is not covered in the proposed CIP Reliability Standards, and is therefore left to the discretion of each responsible entity.

In general, the Commission supports the use of information technology to reduce burden.

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.

The Commission periodically reviews filing requirements concurrent with OMB review or as the Commission deems necessary to eliminate duplicative filing and to minimize the filing burden.

The information collection requirements are unique to this reliability standard and to this information collection. The Commission does not know of any duplication in the requirements.

5. METHODS USED TO MINIMIZE BURDEN IN COLLECTION OF INFORMATION INVOLVING SMALL ENTITIES

The revised CIP Reliability Standards generally do apply to small entities, depending first on their registered function(s) and then on the types of facilities they own. Nearly all of the small entities, which are subject to the CIP version 5 standards, own *only* facilities that should fall into the Low impact category for these standards. This means the burden for these entities is relatively minor compared with the rest of the applicable entities. The only requirements in the revised CIP Reliability Standards that are applicable to most small entities are CIP-002-5.1 (BES Cyber System Categorization) and CIP-003-6 (Security Management Controls, Low impact Policies and Low impact BES cyber system plans).

Using the list of assets containing Low Impact BES Cyber Systems from CIP-002, the intent of CIP-003-6 Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that addresses objective criteria for the protection of Low Impact BES Cyber Systems. The protections required by Requirement R2 reflect the level of risk that must use Guidelines and Technical Basis or the unavailability of Low Impact BES Cyber Systems poses to the BES. The intent is that the required protections are part of a program that covers the Low Impact BES Cyber Systems collectively either at an asset or site level (assets containing low impact BES Cyber Systems), but not at an individual device or system level. There are four subject

matter areas, as identified in Attachment 1, that must be covered by the cyber security plan: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls for LERC and Dial-up Connectivity, and (4) Cyber Security Incident response. .

NERC's Standard Drafting Team of technical experts considered the impact on small entities when setting the cyber asset impact classification levels and intended that the Low Impact BES Cyber Assets would be provided with the least effort and cost, compared to other impact levels. For example, the revised CIP Reliability Standards do not require responsible entities to: (1) maintain comprehensive inventories of all Low Impact BES Cyber Systems, (2) implement specific technical controls for each low impact BES cyber system, (3) maintain lists of recipients and track the reception of the awareness material by personnel, (4) specify a need for each access or authorization of a user to access Low Impact BES Cyber Systems, (5) implement monitoring for each Low Impact BES Cyber System or site, (5) establish a Low Impact Electronic Access Point for each Low Impact BES cyber system. The low impact controls in CIP-003-6 Requirement R2 Attachment 1 also contain an exclusion for "point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems," to ameliorate reporting responsibilities for this type of connectivity.

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

The documentation related to the CIP Reliability Standards is an integral part of establishing and maintaining cyber security. The power grid would be at greater risk to cyber threats if the collection was conducted less frequently.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

There is one special circumstances as described in 5 CFR 1320.5(d)(2) related to this information collection.

Entities may have to submit to or show the auditors security or confidential information that is related to the CIP standards. The general practice is that the auditor often does not remove the information from the site of the entity and, in any case, returns the confidential information to the entity following the audit.[2]

[2] This information is based on FERC staff experience with reliability standards.

This special circumstance is necessary to maintain an effective cyber-security program.

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

The ERO process to establish Reliability Standards is a collaborative process with the ERO, Regional Entities, and other stakeholders developing and reviewing drafts and providing comments. The reliability standard was submitted to the FERC for review and approval. In addition, 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 approved collection of data. The NOPR was published in the Federal Register on 7/22/2015 (80 FR 43354).

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

There are no payments or gifts to respondents associated with this collection.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

As stated in item #7, if a registered entity is required to disclose security or confidential information during an audit, the general practice is that the auditor returns that information to the entity following the audit.[3]

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.

There are no questions of a sensitive nature in the reporting requirements.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

The NERC Compliance Registry, as of June 2015, identifies approximately 1,435 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,363 entities will face an increased paperwork burden under the proposed CIP Reliability Standards, and we estimate that a majority of these entities will

[3] See item #7 in this supporting statement.

have one or more Low Impact assets. In addition, we estimate that approximately 23 percent of the entities have assets that will be subject to Reliability Standards CIP-006-6 and CIP-010-2. Based on these assumptions, we estimate the following reporting burden:

Registered Entities	Number of Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets	313	75,120	130,208	130,208
Totals	313	75,120	130,208	130,208

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

- Year 1: Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets: 313 x 240 hrs/entity * $76/hour = $5,709,120
- Years 2 and 3: 313 entities x 416 hrs/entity * $76/hour = $9,895,808 per year.
- The paper work burden estimate includes costs associated with the initial development of a policy to address requirements relating to transient devices, as well as the ongoing data collection burden. 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.

Registered Entities	**Number of Entities**	**Total Burden Hours in Year 1**	**Total Burden Hours in Year 2**	**Total Burden Hours in Year 3**
Entities subject to CIP-003-6 with low impact	1,363	163,560	283,504	283,504

Assets				
Totals	1,363	163,560	283,504	283,504

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

- Year 1: Entities subject to CIP-003-6 with Low Impact Assets: 1,363 x 120 hrs/entity * $76/hour = $12,430,560.
- Years 2 and 3: 1,363 entities x 208 hrs/entity * $76/hour = $21,546,304 per year.
- The paper work burden estimate includes costs associated with the modification of existing policies to address requirements relating to low impact assets, as well as the ongoing data collection burden, as set forth in CIP-003-6, Requirements R1.2 and R2, and Attachment 1. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to revising existing policies, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

The total burden hours are 355,367.

For Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets, the average of the burden hours of year 1, year 2, and year 3 is111,845 hours.

- 75,120 + 130,208 + 130,208 = 335,536 /3 = 111,845

For Entities subject to CIP-003-6 with low impact Assets, the average of the burden hours of year 1, year 2 and year 3 is 243,522 hours.

- 163,560 + 283,504 + 283,504 = 730,568 / 3 = 243,522

Proposed standards CIP-004-6, -007-6, 009-6, and -011-2 do not affect burden.

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 proposed 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 estimated annualized cost to the Federal Government for FERC-725B as related to the requirements in the NOPR in RM15-14-000 follows:

Annualized cost to Federal Government

	Number of Employees (FTE)	**Estimated Annual Federal Cost**
FERC-725B Analysis and Processing of filings	0	$0
PRA[4] Administrative Cost[5]		$5,193
FERC Total		$5,193

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

The Federal Energy Regulatory Commission (Commission) proposes to approve seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). The North American Electric Reliability Corporation (NERC) submitted the proposed Reliability Standards in response to the Commission's Order No. 791. The proposed Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the

[4] Paperwork Reduction Act of 1995 (PRA)

[5] 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 (not just the NOPR in Docket No. RM15-14-000), and other changes to the collection.

Commission proposes to direct NERC to develop certain modifications to Reliability Standard CIP-006-6 and to develop requirements addressing supply chain management.

The proposed Reliability Standards are designed to mitigate the cybersecurity risks to bulk electric system facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cybersecurity incident, would affect the reliable operation of the Bulk-Power System. 3 As discussed below, we believe that the proposed CIP Reliability Standards are just and reasonable and address the directives in Order No. 791 by: (1) eliminating the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements; (2) providing enhanced security controls for Low Impact assets; (3) providing controls to address the risks posed by transient electronic devices (e.g., thumb drives and laptop computers); and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks." Accordingly, we propose to approve the proposed CIP Reliability Standards because they improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards.

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	1415	1415	0	0
Annual Time Burden (Hr)	1,569,409	1,214,042	0	355,367
Annual Cost Burden ($)	0	0	0	0

16. TIME SCHEDULE FOR PUBLICATION OF DATA

FERC does not publish any data associated with this collection.

17. DISPLAY OF EXPIRATION DATE

It is not appropriate to display the expiration date for OMB approval of the information collected pursuant to this rulemaking affecting FERC-725B because there are no specific instruments used in the collection.

The expiration date is displayed at http://www.ferc.gov/docs-filing/info-collections.asp.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.