SUPPORTING STATEMENT FOR FERC-725B, Revised Critical Infrastructure Protection Reliability Standards, as revised by the Final Rule in Docket No. RM15-14-000

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, as revised and implemented in the Final Rule in Docket No. RM15-14-000.[1]

In this Final Rule (Order No. 822) in Docket RM15-14, the Commission approves seven revised Critical Infrastructure Protection (CIP) Reliability Standards:

1. CIP-003-6 (Security Management Controls)
2. CIP-004-6 (Personnel and Training)
3. CIP-006-6 (Physical Security of BES Cyber Systems)
4. CIP-007-6 (Systems Security Management)
5. CIP-009-6 (Recovery Plans for BES Cyber Systems)
6. CIP-010-2 (Configuration Change Management and Vulnerability Assessments)
7. CIP-011-2 (Information Protection).

The new Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards (CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1, which are being retired).

FERC-725B (OMB Control No. 1902-0248) is an existing data collection, as contained in 18 Code of Federal Regulations (CFR), Part 40. The Final Rule in RM15-14 makes changes discussed below.

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.[2] 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

[1] The Final Rule (Order No. 822) is available in FERC's eLibrary at http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=14124493 ; the News Release is posted at http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=14124226 .

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.[3] The Reliability Standards in RM15-14 address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the Commission directs NERC to develop certain modifications to improve the CIP Reliability Standards to: (1) address the protection of transient electronic devices used at Low Impact BES Cyber Systems, (2) develop modifications to CIP-006-6 to require protections for communication network components and data communicated between all bulk electric system Control Centers according to the risk posed to the bulk electric system, and (3) develop modifications to its definition for Low Impact External Routable Connectivity.

The new versions of the Reliability Standards (noted above) improve upon the current Commission-approved Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1, which are being retired.

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 CIP standards apply to entities registered with the following functional roles: 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 and affected by these CIP Standards. Each of these entities is considered a "respondent" for the purposes of fulfilling the paperwork requirements.

---

[2] 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).

[3] Order Nos. 791 and 791A are available at http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=13398919 and http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=13487724 .

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 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 that in Years 1-3, the PRA-type of burden for these entities is only 50% of the burden for entities with Medium or High Impact.[4] 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)[5] 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

---

[4] The cost related to non-PRA items is much higher for Low Impact entities in Year 1, but they have no ongoing cost in subsequent years.

[5] Reliability Standard CIP-002-5.1 is a scoping standard, which describes how to categorize BES Cyber Systems; it is not affected by the final rule in RM15-14.

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 for the bulk electric system. 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 are special circumstances as described in 5 CFR 1320.5(d)(2) related to this information collection.

Security or Confidentiality. 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.[6]

Records Retention. Audits are periodically conducted on responsible entities based on their risk to the bulk electric system, (generally between 3-6 years for most entities). Reliability Standards CIP-003-6 (Cyber Security -Security Management Controls), CIP-006-6 (Cyber Security - Physical Security of BES Cyber Systems), and CIP-010-2 (Cyber Security - Configuration Change Management and Vulnerability Assessments) include

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

the following record retention requirements which may require keeping information longer than 3 years if an entity had been found non-compliant.

Evidence Retention:

The following evidence retention periods 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:

- Each Responsible Entity shall retain evidence of each requirement in this 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….

These special circumstances are 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.[7] The reliability standards were 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,

[7] Details of the ERO standards development process are available on the NERC website at http://www.nerc.com/docs/standards/sc/Standard_Processes_Manual_Approved_May_2010.pdf.

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).

The Commission received no comments regarding the need for the information collection or the burden estimates (or other PRA-related issues).

All public comments (which in this case are not PRA-related) are addressed in the Final Rule.

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 above, 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. In addition, 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 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 under FERC-725B to FERC. Rather, they 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.

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

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION[9]

[8] Section 1502, Paragraph 2, available at NERCs website.

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 of 1,435 entities, we estimate that 1,363 entities[10] will face an increased paperwork burden under the new CIP Reliability Standards addressed in the Final Rule in Docket RM15-14, and we estimate that a majority of these entities[11] will have one or more Low Impact assets. In addition, we estimate that approximately 23 percent of the 1,363 entities (or 313 entities) will have medium and or/high impact assets that will be subject to Reliability Standards CIP-006-6 and CIP-010-2.

Entities with Medium and/or High Impact Assets. Based on these assumptions, we estimate the following reporting burden for entities with Medium and/or High Impact Assets:

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

[9] The estimated hourly rate of $76 is the average (rounded) loaded cost (wages plus benefits) of legal services ($129.68 per hour), technical employees ($58.17 per hour) and administrative support ($39.12 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics. See http://bls.gov/oes/current/naics2_22.htm and http://www.bls.gov/news.release/ecec.nr0.htm, hourly figures as of June 1, 2015.

[10] The types of entities affected [based on their roles (e.g., Balancing Authority, Distribution Provider, etc.) and certain criteria] are identified in each standard under the Applicability section.

[11] To be conservative, we are assuming the entire group of 1,363 entities affected by these CIP Standards has low impact assets subject to CIP-003-6, as shown in the table below.

Totals[12]	313	75,120	130,208	130,208

The following shows the annual cost burden for the group with Medium and/or High Impact Assets, 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 entities 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 paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to transient electronic devices, as well as the ongoing data collection burden.
  Note that the estimates reflect 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.

Entities with Low Impact Assets. Based on the assumptions, we estimate the following reporting burden for entities with Low Impact Assets:

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 Assets	1,363	163,560	283,504	283,504
Totals[13]	1,363	163,560	283,504	283,504

- The following shows the annual cost burden for the group with Low Impact Assets, based on the burden hours in the table above: Year 1: Entities subject to

[12] For Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets, the average annual burden hours for Years 1-3 is 111,845 hours ((75,120 + 130,208 + 130,208)/3 = 111,845 hrs.), rounded.

[13] For Entities subject to CIP-003-6 with low impact Assets, the average annual burden hours for Years 1-3 is 243,523 hours ((163,560 + 283,504 + 283,504)/ 3 = 243,522 hrs.), rounded.

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.
  Note that the estimates reflect 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.

Other Standards. Reliability Standards CIP-004-6, -007-6, -009-6, and -011-2 do not affect burden.

Summary. The total effect on burden of the Final Rule in RM15-14 over Years 1-3 is:

Registered Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Affected entities with Medium and/or High Impact Assets	75,120	130,208	130,208
Affected entities with Low Impact Assets	163,560	283,504	283,504
Total burden change, due to RM15-14[14]	+238,680	+413,712	+413,712

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

There are no start-up or other non-labor costs for PRA-related items. For example, respondents will not have to buy new storage hardware/software or increase warehouse rental space due to updated versions of these standards.

Total Capital and Start-up cost: $0
Total Operation, Maintenance, and Purchase of Services: $0

[14] The average annual burden increase over Years 1-3 due to the Final Rule in RM15-14 is 355,368 hours (the figure which will be shown in ROCIS and reginfo.gov metadata).

All of the PRA-related costs in the final rule are associated with burden hours (labor) and are 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 Final Rule in RM15-14-000 follows:

	Number of Employees (FTE)	**Estimated Annual Federal Cost**
FERC-725B Analysis and Processing of filings	0	$0
PRA[15] Administrative Cost[16]		$5,193
FERC Total		$5,193

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

In this Final Rule, FERC approves 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).

[15] Paperwork Reduction Act of 1995 (PRA)

[16] 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 this rulemaking), and other changes to the collection.

On 2/13/2015, NERC submitted the proposed Reliability Standards in response to the Commission's Order No. 791. NERC's Petition stated in part [footnotes omitted]:

> "The purpose of NERC's CIP cybersecurity Reliability Standards is 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 cyber-attack, would affect the reliable operation of the Bulk Electric System. On November 22, 2013, the Commission issued Order No. 791, approving new and modified CIP cybersecurity Reliability Standards, collectively referred to as the CIP Version 5 Standards, to become effective on April 1, 2016. As the Commission stated, the CIP Version 5 Standards represent an improvement over the currently-effective CIP Reliability Standards as they adopt new cybersecurity controls and extend the scope of the systems protected by the CIP Reliability Standards. While the Commission approved the CIP Version 5 Standards, it also directed NERC to develop the following modifications to improve those standards:
>
> 1. Modify or remove the language in 17 requirements in the CIP Version 5 Standards that requires responsible entities to implement cyber security policies in a manner that "identifies, assesses, and corrects deficiencies."
> 2. Develop modifications to the CIP Version 5 Standards to address security controls for low impact BES Cyber Systems.
> 3. Develop requirements that protect transient devices (e.g., thumb drives, laptop computers, and other devices that are portable and frequently connected and disconnected from systems on a temporary basis) that fall outside the definitions for BES Cyber Asset and PCA.
> 4. Create a definition of "communication networks" and develop new or modified standards that address the protection of the nonprogrammable components of communication networks.
>
> The Commission directed NERC to submit for Commission approval revised standards addressing the "identify, assess, and correct" and communication networks directives within one year from the effective date of Order No. 791…. The Commission did not provide a deadline for the directives related to low impact BES Cyber Systems and transient devices.
>
> As discussed further below, the proposed Reliability Standards improve the cybersecurity protections required by the CIP Reliability Standards…."

The Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition in this order, the Commission directs NERC to develop certain modifications to improve further the CIP Reliability Standards.

The CIP 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. FERC finds that the 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) used at High and Medium Impact BES Cyber Systems; and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks." Accordingly, the Commission approves the CIP Reliability Standards because they improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards. FERC also directed NERC to develop certain modifications as discussed in the order.[17]

The change to the burden inventory due to implementation of the Final Rule in RM15-14 follows.

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	1,415	1,415	0	0
Annual Time Burden	1,569,410	1,214,042	0	+355,368[18]

[17]In the NOPR, FERC also proposed to direct that NERC develop requirements relating to supply chain management for industrial control system hardware, software, and services. After review of comments on this topic, the Commission scheduled a staff-led technical conference for January 28, 2016, in order to facilitate a structured dialogue on supply chain risk management issues identified by the NOPR. Accordingly, this Final Rule does not address supply chain risk management issues. Rather, the Commission will determine the appropriate action on this issue after the scheduled technical conference.

(Hr.)				
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

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.

[18] The average annual burden increase over Years 1-3 due to the Final Rule in RM15-14 is 355,368 hours.