FERC-725B, OMB Control No. 1902-0248

Final Rule in Docket RM11-11 (issued 4/19/2012); RIN 1902-AE41

Supporting Statement for

FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection

(As modified in the Final Rule in Docket No. RM11-11, issued April 19, 2012)

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) approve **FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection (CIP)**, for the revisions to the Reliability Standards found in the Final Rule in Docket No. RM11-11. FERC-725B[1] (OMB Control No. 1902-0248) is an existing data collection, as contained in 18 Code of Federal Regulations (CFR), Part 40.

Final Rule in RM11-11

In this Final Rule, FERC approves Version 4 of the Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-4 through CIP-009-4. The Version 4 CIP Reliability Standards were developed and submitted by the North American Electric Reliability Corporation (NERC) to FERC for approval. In general, the CIP Reliability Standards provide a cybersecurity framework for the identification and protection of Critical Cyber Assets to support the reliable operation of the Bulk-Power System.[2] In particular, the Version 4 CIP Reliability Standards modify CIP-002 to include "bright line" criteria for the identification of Critical Assets, in lieu of the currently-required risk-based assessment methodology that is developed and applied by registered entities. In addition, NERC developed conforming modifications to the remaining CIP Reliability Standards, CIP-003 through CIP-009. The Commission also approves the retirement of the currently effective Version 3 CIP Reliability Standards, CIP-002-3 to CIP-009-3.

A. Justification

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, the Electricity Modernization Act of 2005, which is Title XII, Subtitle A, of the Energy Policy Act of 2005, was enacted.[3] That Act added a new section 215 to the Federal Power Act (FPA), requiring an Electric Reliability Organization (ERO), certified by FERC, to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. These Commission-

1 FERC-725B was last approved by OMB on 9/15/2011 for a 3-year renewal under ICR Ref No. 201104-1902-001. That clearance package reflected the CIP standards through Version 3.

2 The NERC Glossary of Terms defines Critical Assets to mean "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

3 Energy Policy Act of 2005, Pub. L. No 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005); 16 U.S.C. § 824o (2006).

approved Reliability Standards developed by NERC, the Commission-certified ERO, may be enforced by the ERO subject to Commission oversight, or independently enforced by the Commission.

On February 3, 2006, the Commission issued Order No. 672, implementing section 215 of the FPA.[4] Pursuant to Order No. 672, the Commission certified NERC as the ERO.[5] The Reliability Standards developed by the ERO and approved by the Commission will apply to users, owners and operators of the Bulk-Power System, as set forth in each Reliability Standard.

On January 18, 2008, the Commission issued Order No. 706, approving eight CIP Reliability Standards proposed by NERC. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address various concerns discussed in the Final Rule. Specifically, the Commission directed the ERO to address the following issues regarding CIP-002-1: (1) need for ERO guidance regarding the risk-based assessment methodology for identifying Critical Assets; (2) scope of Critical Assets and Critical Cyber Assets; (3) internal, management, approval of the risk-based assessment; (4) external review of Critical Assets identification; and (5) interdependency between Critical Assets of the Bulk-Power System and other critical infrastructures. Subsequently, the Commission approved Version 2 and Version 3 of the CIP Reliability Standards, each version including changes responsive to some, but not all, of the Commission's directives in Order No. 706.

Events that make this collection necessary

A common cause of past major regional blackouts was violation of NERC's then Operating Policies and Planning Standards. A key to the successful cyber protection of the Bulk-Power System is the establishment of CIP Reliability Standards that provide sound, reliable direction on how to choose among alternatives to achieve an adequate level of security, and the flexibility to make those choices. This conclusion is consistent with the lessons learned from the August 2003 blackout occurring in the central and northeastern United States. The identification of the causes of that and other major blackouts helped determine where existing Reliability Standards need modification or new Reliability Standards need to be developed to improve Bulk-Power System reliability. The U.S. – Canada Power System Blackout Task Force, in its Blackout Report, developed specific recommendations for improving the then-current voluntary standards and development of new Reliability Standards.[6]

---

4 Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, Order No. 672, 71 FR 8662 (Feb. 17, 2006), FERC Stats. & Regs. ¶ 31,204 (2006), order on reh'g, Order No. 672-A, 71 FR 19814 (Apr. 18, 2006), FERC Stats. & Regs. ¶ 31,212 (2006).

5 North American Electric Reliability Corp., 116 FERC ¶ 61,062 (ERO Certification Order), order on reh'g & compliance, 117 FERC ¶ 61,126 (ERO Rehearing Order) (2006), order on compliance, 118 FERC ¶ 61,030 (2007) (Jan. 2007 Compliance Order), appeal docket sub nom. Alcoa, Inc. v. FERC, No. 06-1426 (D.C. Cir. Dec. 29, 2006).

6 U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United

Final Rule in Docket RM11-11 (issued 4/19/2012); RIN 1902-AE41

Thirteen of the 46 Blackout Report Recommendations relate to cyber security. They address topics such as: (1) the development of cyber security policies and procedures; (2) strict control of physical and electronic access to operationally sensitive equipment; (3) assessment of cyber security risks and vulnerability at regular intervals; (4) capability to detect wireless and remote wireline intrusion and surveillance; (5) guidance on employee background checks; (5) procedures to prevent or mitigate inappropriate disclosure of information; and, (6) improvement and maintenance of cyber forensic and diagnostic capabilities.[7] The CIP Reliability Standards address these and other related topics.

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

How is the information used?

Under CIP-002-4, registered entities create lists of Critical Assets and Critical Cyber Assets. Entities that identify Critical Cyber Assets must meet the requirements of CIP-003-4 through CIP-009-4. These latter standards deal with areas such as personnel training, systems security and physical perimeter security. In all cases entities generate documentation that they keep to show compliance with the requirements of the standards

Who uses the information?

The registered entity uses the information to demonstrate compliance. The compliance enforcement authority reviews the information.

Why is the information collected?

The registered entities document the policies, plans, programs and procedures to clearly show compliance with the CIP Reliability Standards.

What are the consequences of not collecting the information?

Without this documentation, the compliance enforcement authority would have difficulty in verifying compliance with the CIP Reliability Standards. Without the ability to verify compliance with the CIP Reliability Standards, serious breaches in cyber security could result and compromise the reliable operation of the Bulk-Power System.

States and Canada: Causes and Recommendations (April 2004) (Blackout Report). The Blackout Report is available on the Internet at https://reports.energy.gov/BlackoutFinal-Web.pdf.

7 See Blackout Report at 163-169, Recommendations 32-44.

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

The CIP Reliability Standards require entities to document compliance with the requirements. In this effort, the Commission supports the use of improved technology and improved processes to reduce the burden of complying with CIP Reliability Standard requirements.

The Commission approves in this version of the standards bright line criteria for identifying cyber assets. This eases the burden on entities that, under the previous version of the standards, had to create a methodology for determining cyber assets.

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 responsibilities under the FPA in order to eliminate duplication and ensure that filing burden is minimized. There are no similar sources of 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 rule may significantly impact several small entities. While the Commission recognizes this impact, the Commission is also concerned that Bulk-Power System reliability not be compromised based on an unwillingness of entities, large or small, to incur reasonable expenditures necessary to preserve such reliability.

The Commission allows small entities to join a joint action agency or similar organization, which could accept responsibility for compliance with the Reliability Standards on behalf of its members.

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

If the collection requirements were imposed less frequently, the compliance enforcement authority would have difficulty in keeping up to date regarding compliance with the CIP Reliability Standards. Without current verification, serious breaches in cyber security could perpetuate and potentially compromise the reliable operation of the Bulk-Power System.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

The guidelines of 5 C.F.R. 1320.5(d) are being followed.

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

The Commission's procedures require that the rulemaking notice be published in the Federal Register, thereby allowing all pipeline companies, state commissions, federal agencies, and other interested parties an opportunity to submit comments, or suggestions concerning the proposal. The Notice of Proposed Rulemaking (NOPR) in this proceeding solicited public comments. In response to the NOPR, comments were filed by 28 interested entities.

Hydro-Québec TransÉnergie (Hydro-Québec) and Sierra Pacific Power Company and Nevada Power Company (NV Energy) submitted comments related directly to the burden/cost estimates.

Comments

Hydro-Québec and NV Energy claim that the cost estimates included in the NOPR for Version 4 are inaccurate and incomplete.[8] NV Energy states that the estimate does not include the significant burden of the additional security requirements that will be required by the identification of more Critical Assets and related Critical Cyber Assets. NV Energy comments that the cost estimate does not consider such matters as increased background checking, personnel risk assessments, cyber security training programs, and increased complexity of cyber security perimeters.

Commission Determination

After a review of the comments on the Commission's cost estimate, we maintain the cost estimate provided in the NOPR. While we recognize that implementing the Reliability Standards is not without cost, the benefits to reliability must be recognized. In response to Hydro-Québec and NV Energy's concerns, we note that the estimate provided in the NOPR addresses the potential for an incremental increase in costs across the industry and does not address the full cost of implementing the CIP Reliability Standards by an entity. We anticipate that the savings associated with the change from the entity-specific risk-based assessment methodology, which had to be reviewed and updated each year, to a bright-line approach will offset some, if not all, of the incremental

8 Hydro-Québec Comments at 6; NV Energy Comments at 6-7. All comments related to this rulemaking can be found through the Commission's eLibrary site (http://www.ferc.gov/docs-filing/elibrary.asp) by searching on Docket No. RM11-11.

cost increase for entities that have previously identified a Critical Cyber Asset. With regards to NV Energy's comments, we note that the revisions to the Version 4 CIP Reliability Standards address the manner for the identification of Critical Assets, and do not revise current requirements pertaining to background checking, personnel risk assessments, cyber security training programs, and cyber security perimeters.

Other Comments (not directly related to burden/cost) and the Commission's Response

We discuss all other comments and provide responses in the preamble to the final rule. The final rule can be downloaded from the Commission's eLibrary site at http://www.ferc.gov/docs-filing/elibrary.asp by searching on Docket No. RM11-11. Also, we attached in ROCIS under the public comment section an excerpted portion from the rule containing a summary of these comments and the Commission's full response.

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

The Commission generally does not consider the data to be confidential. However, certain CIP Reliability Standards may have confidentiality provisions in the standard.

The Commission has in place procedures to prevent the disclosure of sensitive information, such as the use of protective orders and rules establishing critical energy infrastructure information (CEII). However, the Commission believes that the specific, limited area of Cyber Security Incidents requires additional protections because it is possible that system security and reliability would be further jeopardized by the public dissemination of information involving incidents that compromised the cybersecurity system of a specific user, owner or operator of the Bulk-Power System. In addition, additional information provided with a filing may be submitted with a specific request for confidential treatment to the extent permitted by law and considered pursuant to 18 C.F.R. 388.112 of FERC's regulations.

11. PROVIDE ADDITIONAL JUSTIFICATION FOR ANY QUESTIONS OF A SENSITIVE NATURE THAT ARE CONSIDERED PRIVATE.

There are no questions of a sensitive nature that are considered private.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

Burden impact of the rule

FERC-725B, OMB Control No. 1902-0248

Final Rule in Docket RM11-11 (issued 4/19/2012); RIN 1902-AE41

The Commission estimates the final rule will add a net of 30,840 hours to the respondents of the FERC-725B collection as follows:

- Entities that identify at least one Critical Cyber Asset [category a]:
    - Reduction of 40 hours per response (345 responses X 40 hrs/response = 13,800 hours reduction)
- Entities not identifying Critical Cyber Assets [category b]:
    - Reduction of 12 responses (12 responses X 120 hrs/response = 1,440 hours reduction)
- Entities identifying for the first time Critical Assets/Critical Cyber Assets [category c]:
    - Addition of 12 responses (12 responses X 3,840 hrs/response = 46,080 hours addition)

Background on number of respondents

The Commission used the NERC Compliance Registry as of 9/28/2010 that indicated that 2,079 entities were registered for NERC's compliance program. Of these, 2,057 were identified as being U.S. entities. Staff concluded that of the 2,057 U.S. entities, approximately 1,501 were registered for at least one CIP related function. According to an April 7, 2009 memo to industry, NERC noted that only 31% of entities responding to an earlier survey reported that they had at least one Critical Asset, and only 23% reported having a Critical Cyber Asset. Staff applied the 23% (an estimate unchanged for Version 4 standards) to the 1,501 figure to estimate the number of entities that identified Critical Assets under Version 3 CIP Standards.

Total burden (including the impacts of the final rule)

The following table breaks out the burden by groups of registered entities. Rows 2 through 5 include a category classification that is used in the detailed burden assumptions shown below the table.

Total FERC-725B Burden					
Registered Entities	**Number of Respondents (A)**	**Number of Responses Per Respondent (B)**	**Total Number of Responses (A)x(B)=(C)**	**Average Burden Hours per Response (D)**	**Estimated Total Annual Burden (C)x(D)**
Entities that identify at least one critical cyber asset [category a]	345	1	345	1,880	648,600
Entities not identifying	1,144	1	1,144	120	137,280

critical cyber assets [category b]					
Entities identifying for the first time cyber assets/critical cyber assets [category c][9]	18	1	18	3,840	69,120
Entities no longer required to comply with CIP standards [category d][10]	-6	1	-6	720	-4,320
TOTAL	1,501	N/A	1,501	N/A	850,680

Assumptions used for the burden hours per response figures (column D from table above)

- Respondent category a
    - 50% of the time it takes for entities identifying cyber assets/critical cyber assets for the first time (50% of 3,840 hours = 1920 hours).
    - This rule further assumes a 40 hour reduction in the category (1,920 hours - 40 hours = 1,880 hours)
- Respondent category b
    - 3 employees, each spending 20 hours a week for two weeks (3 X 20 hours/week X 2 weeks = 120 hours)
- Respondent category c
    - 20 employees, each spending 20 hours a week for eight weeks (20 X 20 hours/week X 8 weeks = 3,200 hours)
    - Plus, additional hours equal to 20% of the burden on the 20 employees (20% of 3,200 hours = 640 hours => 640 hours + 3200 hours = 3,840 hours
- Respondent category d
    - This represents the net reduction in hours assuming 2 entities dropping out of category a and 4 entities dropping out of category b [(2 X 1,920 hours

9 Of the 18 entities in this category, 12 are brought in because of the new requirements in the final rule, and the other six represent the new entities that would have to comply with the CIP standards in a given year (independent of the final rule). After the initial audit cycle it is assumed that two of these six entities will be accounted for in category a and the other four in category b. This addition to categories a and b corresponds to the removal of category d entities. The 12 new entities brought on because of the rule will also become part of categories a and b after the initial audit cycle.

10 These six entities are not dropping out because of any new requirements associated with the rule. It is assumed that these six entities represent those that leave the industry for whatever reason.

[burden per response for category b prior to the rule because those dropping out will not experience the burden reduction]) + (4 X 120 hours) = 4,320hours. 4,320 hours/6 responses = 720 (rounded) average hours/response

Burden Summary

The following table summarizes the changes due to the rule and shows how the new burden inventory compares to the old burden inventory.

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	1,501	1,501	-	-
Annual Time Burden (Hr)	850,680	819,840	-	30,840
Annual Cost Burden ($)	$5,444	$5,261	-	$183

All of the burden associated with monitoring and enforcing compliance of the CIP Reliability Standards (typically carried out by regional entities or NERC) are contained in FERC-725 (OMB Control No. 1902-0225) and are not part of this collection. This collection only contains the burden on the registered entities for complying with the direct requirements of the standards.

13. **ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS**

Revisions to the cost estimates based on the requirements of the rule:

- Each entity that has identified Critical Cyber Assets (category a) has a program change reduction of 40 hours, providing a total cost reduction of $1,324,800 (or 345 entities X 40 hours X $96/hour).
- 12 Entities that formerly had not identified Critical Cyber Assets, but will now have them (formerly in category b, and now going to category c) have a program change of:
  - A reduction of 120 hours per entity and an increase of 3,840 hours per entity, for a net increase of 3,720 annual hours per entity. This results in $4,285,440 increase (12 entities X 3,720 hours X $96/hour).
  - Storage costs = 12 entities X $15.25/entity = $183 increase.

Total Net Annual Cost Increase for the FERC-725B requirements contained in the final rule = $2,960,823 (-$1,324,800 + $4,285,440 + $183).

Final Rule in Docket RM11-11 (issued 4/19/2012); RIN 1902-AE41

The estimated hourly rate of $96 is the average cost of legal services ($230 per hour), technical employees ($40 per hour) and administrative support ($18 per hour), based on hourly rates from the Bureau of Labor Statistics (BLS) and the 2009 Billing Rates and Practices Survey Report.[11] The $15.25 per entity for storage costs is an estimate based on the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Reliability Standards.[12]

Total FERC-725B annual cost burden after implementation of the rule:

$81,678,404 ($78,717,581 for the existing requirements, plus $2,960,823 for the changes from the final rule).

The total cost for the recordkeeping requirements would be $5,444 (or the $5,261 from the current OMB inventory + $183 from the final rule). The $5,444 is included in the $81,678,404.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The estimate of the cost to the Federal Government is based on salaries and benefits for professional and clerical support.

The CIP Reliability Standards do not require any information to be submitted to FERC. Most of the burden on FERC pertaining to the CIP standards relates to violation reporting or other compliance monitoring and review activities, all of which are contained in the FERC-725 collection (OMB Control No. 1902-0225). FERC does incur costs in maintaining this collection of information current with OMB as is estimated here:

Data Clearance Program: $1,588

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

In the final rule FERC adopts revisions to eight CIP Reliability Standards that include a new method of identifying cyber assets that are critical to the nation's Bulk-Power System.

The new Version 4 CIP Reliability Standards replace the existing risk-based assessment methodology for identifying Critical Assets with 17 uniform "bright line" criteria, making the process more consistent and clear by limiting discretion in the identification of such assets.

11 Bureau of Labor Statistics figures were obtained from http://www.bls.gov/oes/current/naics2_22.htm, and 2009 Billing Rates figure were obtained from http://www.marylandlawyerblog.com/2009/07/average_hourly_rate_for_lawyer.html. Legal services were based on the national average billing rate (contracting out) from the above report and BLS hourly earnings (in-house personnel). It is assumed that 25% of respondents have in-house legal personnel.

12 Based on the aggregate cost of an advanced data protection server.

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

Commission-approved reliability standards are available on the ERO's website at http://www.nerc.com/page.php?cid=2|20. There is no publication of the FERC-725B data.

17. DISPLAY OF THE EXPIRATION DATE

It is not appropriate to display the expiration date for OMB approval of the information collected. The information will not be collected on a standard, preprinted form which would avail itself to that display.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

The data collected for this reporting requirement is not used for statistical purposes. Therefore, the Commission does not use as stated in item (i) on the certification statement, "effective and efficient statistical survey methodology." The information collected is case specific to each CIP Reliability Standard.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS.

This is not a collection of information employing statistical methods.