FERC-725B, OMB Control No. 1902-0248
[updated 10/31/2011]
NOPR in Docket RM11-11 (issued 9/15/2011); RIN 1902-AE41

Supporting Statement for

FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection (as modified in NOPR in Docket No. RM11-11, issued 9/15/2011)

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 proposed revisions to the Reliability Standards found in the Notice of Proposed Rulemaking (NOPR) 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.

The CIP Reliability Standards are necessary to support the reliable operation of the Bulk-Power System.

Background

In the aftermath of the 1965 Blackout in the northeast United States, the electric industry established the North American Electric Reliability Council (NERC), a voluntary reliability organization. Since its inception, NERC has developed Operating Policies and Planning Standards that provide voluntary guidelines for operating and planning the North American Bulk-Power System. In April 2005, NERC adopted "Version O" Reliability Standards that translated the NERC Operating Policies, Planning Standards and compliance requirements into a comprehensible set of measurable Reliability Standards. While NERC has developed a compliance management and enforcement program to ensure compliance with the Reliability Standards it developed, industry compliance has been voluntary and not subject to mandatory enforcement penalties.

On August 8, 2005, the Electricity Modernization Act of 2005, which is Title XII, Subtitle A, of the Energy Policy Act of 2005 (EPAct 2005), was enacted into law.[2] EPAct 2005 adds a new section 215 to the 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, or the Commission can independently enforce Reliability Standards.[3]

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

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 one organization, 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. In relevant part, 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.

NOPR in RM11-11. In this NOPR in RM11-11, FERC proposes to approve Version 4 of the CIP Reliability Standards, CIP-002-4 through CIP-009-4. The proposed Version 4 CIP Reliability Standards were developed and submitted by 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.[6] In particular, the Version 4 CIP Reliability Standards propose to modify CIP-002-4 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 proposed conforming modifications to the remaining CIP Reliability Standards, CIP-003-4 through CIP-009-4.

FERC proposes to approve Version 4 of the CIP Reliability Standards, the Violation Risk Factors (VRFs) and the Violation Severity Levels (VSLs) with

---

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 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."

modifications, the associated implementation plan, and the effective date for Version 4 CIP Reliability Standards as proposed by NERC. The Commission also proposes to approve the retirement of the currently effective Version 3 CIP Reliability Standards, CIP-002-3 to CIP-009-3.

While FERC proposes to approve the Version 4 CIP Standards, like NERC, the Commission recognizes that the Version 4 CIP Standards represent an "interim step"[7] to addressing all of the outstanding directives set forth in Order No. 706.[8] The Commission believes that the electric industry, through the NERC standards development process, should continue to develop an approach to cybersecurity that is meaningful and comprehensive to assure that the nation's electric grid is capable of withstanding a Cybersecurity Incident.[9] FERC expects NERC will continue to improve the CIP Reliability Standards and to address all outstanding directives in Order No. 706.

A. Justification

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

EPAct 2005 added a new section 215 to the FPA, which provides for a system of mandatory and enforceable Reliability Standards. Section 215(d)(1) of the FPA provides that the ERO must file each Reliability Standard or modification to a Reliability Standard that it proposes to be made effective (i.e., mandatory and enforceable) with the Commission. As mentioned above, on August 28, 2006, NERC submitted eight CIP Reliability Standards for Commission approval pursuant to section 215(d) of the FPA. As NERC continues to revise the CIP Reliability Standards pursuant to section 215(d) of the FPA, compliance information must be collected and/or retained by NERC and the eight Regional Entities to demonstrate that registered entities are protecting both the physical assets, and the critical assets including critical cyber assets of the Bulk-Power System.

Some Triggering Events

A common cause of past major regional blackouts was violation of NERC's then Operating Policies and Planning Standards. During July and August 1996, the west coast of the United States experienced two cascading blackouts caused by violations of

7 NERC Petition at 6.
8 *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009).
9 Section 215(a) of the FPA defines Cybersecurity Incident as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the Bulk-Power System."

voluntary Operating Policies.[10] In response to these outages, the Secretary of Energy convened a task force to advise the Department of Energy (DOE) on issues needed to be addressed to maintain the reliability of the Bulk-Power System. In a September 1998 report, the task force recommended, among other things, that federal legislation should grant more explicit authority for FERC to approve and oversee an organization having responsibility for bulk-power reliability standards.[11] Further, the task force recommended that such legislation provide for FERC jurisdiction for reliability of the Bulk-Power System and FERC implementation of mandatory, enforceable Reliability Standards.

Electric reliability legislation was first proposed after issuance of the September 1998 task force report and continues to be a common feature of comprehensive electricity bills since then. A stand-alone electric reliability bill was passed by the Senate unanimously in 2000. In 2001, then President Bush proposed making electric Reliability Standards mandatory and enforceable as part of the National Energy Policy.[12]

Under the new electric power reliability system enacted by the Congress (EPAct 2005, Section 215 of the FPA), the United States would no longer rely on voluntary compliance by participants in the electric industry with industry reliability requirements for operating and planning the Bulk-Power System. Congress directed the development of mandatory, Commission-approved, enforceable electricity Reliability Standards. The Commission believes that to achieve this goal it is necessary to have a strong ERO that promotes excellence in the development and enforcement of Reliability 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 previous 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.[13]

---

10 The Electric Power Outages in the Western United States, July 2-3, 1996, at 76 (http://www.nerc.com/docs/docs/pubs/doerept.pdf) and WSCC Disturbance Report, For the Power System outage that Occurred on the Western Interconnection August 10, 1996, at 4 (http://www.nerc.com/files/disturb96.pdf).
11 Maintaining Reliability in a Competitive U.S. Electricity Industry, Final report of the Task Force on Electric System Reliability, Secretary of Energy Advisory Board, U.S. Department of Energy (September 1998), at 25-27, 65-67.
12 Report of the National Energy Policy Development Group, May 2001, at p. 7-6.
13 U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United 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.

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.[14] The CIP Reliability Standards address these and other related topics.

As the Commission noted in Order No. 693, the Blackout Report recommendations address key issues for assuring Bulk-Power System reliability and represent a well-reasoned and sound basis for action.[15]

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 the CIP Reliability Standards a registered entity is not required to "report" to the Commission, ERO or the Regional Entities, the various policies, plans, programs and procedures to demonstrate compliance with the CIP Reliability Standards. However, a registered entity is required to "produce" the documented policies, plans, programs and procedures during a periodic compliance audit or spot check for example to demonstrate compliance with the CIP Reliability Standards.

Who uses the information?

The registered entity utilizes the information during a periodic audit to demonstrate compliance with the CIP Reliability Standards.

Why is the information collected?

The registered entities purpose in documenting policies, plans, programs and procedures is to clearly establish for the auditors how the CIP Reliability Standards are being followed.

What are the consequences of not collecting the information?

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

14 See Blackout Report at 163-169, Recommendations 32-44.
15 See Order No. 693 at P 234.

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 do not require a registered entity to report anything to the Commission, ERO or the Regional Entities. However, the Commission supports the use of improved technology and improved processes by registered entities to reduce the burden of complying with CIP Reliability Standard requirements.

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. The filing requirements in FERC-725B will incorporate NERC's filing requirements. However, all reliability filing requirements will be subject to FERC approval along with the filing requirements developed by Regional Entities, Regional Advisory Bodies and the ERO.

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

The Commission believes that Reliability Standards in general may cause some small entities to experience economic impact. While the Commission is mindful of the possible impact on small entities, 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. As the Commission explained in Order No. 672:

> A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a "lowest common denominator" Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example,

a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.[16]

While the Commission cannot rule on the merits until a specific proposal has been submitted, the Commission believes that reasonable limits on applicability based on size may be an acceptable alternative to lessen the economic impact of the proposed rule on small entities. The Commission emphasizes, however, that any such limits must not weaken Bulk-Power System reliability.

The United States Small Business Administration (SBA) established a size standard for electric utilities, stating that a firm is small if, including its affiliates, it is primarily engaged in the transmission, generation and/or distribution of electric energy for sale and its total electric output for the preceding twelve months did not exceed four million megawatt hours.[17]

For the NOPR in RM11-11, FERC analyzed the affect of the proposed rule on small entities. The Commission's analysis found that the DOE's Energy Information Administration (EIA) reports that there were 3,276 electric utility companies in the United States in 2009,[18] and 3,015 of these electric utilities qualify as small entities under the SBA definition. Of these 3,276 electric utility companies, the EIA subdivides them as follows: (1) 875 cooperatives of which 843 are small entity cooperatives; (2) 1,841 municipal utilities, of which 1,826 are small entity municipal utilities; (3) 128 political subdivisions, of which 115 are small entity political subdivisions; (4) 171 power marketers, of which 113 individually could be considered small entity power marketers;[19] (5) 200 privately owned utilities, of which 93 could be considered small entity private utilities; (6) 24 state organizations, of which 14 are small entity state organizations; and (7) 9 federal organizations of which 4 are small entity federal organizations.

Many of the entities that have not previously identified Critical Assets and Critical Cyber Assets are considered small entities. The Version 4 CIP Reliability Standards bright line criteria generally result in the identification of relatively larger Bulk-Power System equipment as Critical Assets. For the most part, the small entities do not own or operate these larger facilities. There is a limited possibility that these entities would have facilities that meet the bright line criteria and therefore be subject to the full CIP standards (CIP-002 through CIP-009). The Commission expects only a marginal increase in the number of small entities that will identify at least one Critical Asset under the Version 4 CIP Reliability Standards that have not done so previously.

---

16 Order No. 672 at P 330.
17 13 CFR 121.201, Sector 22, Utilities & n.1.
18 See Energy Information Administration Database, Form EIA-861, Dept. of Energy (2009), available at http://www.eia.doe.gov/cneaf/electricity/page/eia861.html.
19 Most of these small entity power marketers and private utilities are affiliated with others and, therefore, do not qualify as small entities under the SBA definition.

The Commission estimates that only one percent or 12 of the small and medium-sized entities that have not previously identified Critical Assets and Critical Cyber Assets will have an increased cost due to the Version 4 CIP Reliability Standards and their identification of new Critical Cyber Assets. For each of those 12 small and medium sized entities, we anticipate a cost increase associated with creating a cyber security program along with the actual cyber security protections associated with the identified Critical Cyber Assets. The Commission requests comment on the potential implementation cost and subsequent cost increases that could be experienced by such small entities. Small and medium sized entities that continue to have no Critical Assets will not see any change in their burden.

In general, the majority of small entities are not required to comply with the CIP Reliability Standards because they are not regulated by NERC pursuant to the NERC Registry Criteria. Moreover, a small entity that is registered but does not identify critical cyber assets pursuant to CIP-002-4 will not have compliance obligations pursuant to CIP-003-4 through CIP-009-4.

The Commission also investigated possible alternatives. These included the Commission's adoption in Order No. 693 of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with the Reliability Standards. The Commission also noted that small entities could 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

The ERO conducts periodic assessments of the reliability and adequacy of the Bulk-Power System in North America and reports its findings to the Commission, the Secretary of Energy, the Regional Entities, and the Regional Advisory Bodies annually or more frequently if so ordered by the Commission. The ERO and the Regional Entities report to FERC on their enforcement actions and associated penalties and to the Secretary of Energy, relevant Regional entities and relevant Regional Advisory Bodies annually or quarterly in a manner prescribed by the Commission.

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

FERC-725B is a filing requirement necessary to comply with the applicable provisions of the Electricity Modernization Act of 2005 and section 215 of the Federal Power Act.

There are no special circumstances relating to the information collection.

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. This proposed rule is soliciting public comments.

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

The estimated changes to burden as contained in the proposed rule in RM11-11 follow.

FERC-725B Data Collection (per proposed Version 4)	No. of Respondents[20] (1)	Average No. of Annual Responses Per Respondent (2)	Average No. of Burden Hours Per Response[21] (3)	Effect of NOPR in RM11-11, on Total Annual Hours (1)x(2)x(3)	Annual Burden Hrs. upon Implementation of RM11-11
Entities that (previously and now) will identify at least one Critical Cyber Asset [category a]	345 [no change]	1	1,880 [A reduction of 40 hours from 1,920 to 1,880 hours]	[A reduction of 13,800 hours]	648,600
Entities that (previously and now) will not identify any Critical Cyber Assets	1,144 [A reduction of 12 entities from 1,156 to 1,144]	1	120 [no change]	A reduction of 1,440 hours [for the 12 entities]	137,280

20 The NERC Compliance Registry as of 9/28/2010 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.

21 Calculations for figures:

Respondent category b:

3 employees X (working 50%) X (40 hrs/week) X (2 weeks) = 120 hours

Respondent category c:

20 employees X (working 50%) X (40 hrs/week) X (8 weeks) = 3200 hours
(20%) X (3200 hrs) = 640 hours
Total = 3840

Respondent category a, before reduction proposed in NOPR in RM11-11:

50% of 3840 hours (category d) = 1920
We estimate a reduction of 40 hrs. per response to 1,880 (from 1,920) as a result of the proposal in RM11-11.

[category b]					
Entities that will newly identify a Critical Asset/Critical Cyber Asset due to the requirements in RM11-11[22, 23] [category c]	An increase of 12 [formerly 0]	1	3,840[24]	An increase of 46,080	46,080
Net TotalError: Reference source not found	1,501 Error: Reference source not found			+30,840 [Program change]	831,960Error: Reference source not found
New U.S. Entities that have to come into compliance with the CIP Standards [no change from NOPR in RM11-11] Error: Reference	+6 [no change from NOPR in RM11-11]	1[no change from NOPR in RM11-11]	3,840 [no change from NOPR in RM11-11]	[no change from NOPR in RM11-11]	23,040 [no change from NOPR in RM11-11]

22 We estimate 12 (or 1%) of the existing entities that formerly had no identified Critical Cyber Assets will have them under the proposed Reliability Standards.

23 This proposed rule in RM11-11 does not affect the burden for the 6 new U.S. Entities that were estimated to newly register or otherwise become subject to the CIP Standards each year in FERC-725B, and therefore are not included in this chart.
In the package recently approved by OMB (ICR 201104-1902-001), those 6 "New U.S. Entities that have to come into compliance with the CIP Standards" would have an estimated burden of 3,840 hours per filing (giving an annual estimate of 23,040). In addition, it was estimated that annually 6 "Entities no longer would be required to comply with CIP Standards" (2 category 1 respondents [at 1,920 hrs. each] and 4 category 2 respondents [at 120 hrs. each], giving a reduction of 4,320 hrs.).
Including the net burden related to those 6 entities (18,720 hrs. annually) would raise the estimate of 831,960 [after implementation of RM11-11] to a new total inventory figure of 850,680 annual hrs.

24 This estimated burden estimate applies only to the first three year audit cycle. In subsequent audit cycles these entities will move into category a, or be removed from the burden as an entity that no longer is registered for a CIP related function.

source not found					
Entities no longer would be required to comply with CIP Standards [no change from NOPR in RM11-11] Error: Reference source not found	-6 [no change from NOPR in RM11-11]	1 [no change from NOPR in RM11-11]	2 category 1 respondents [at 1,920 hrs. each] and 4 category 2 respondents [at 120 hrs. each] [no change from NOPR in RM11-11]	[no change from NOPR in RM11-11]	-4,320 [no change from NOPR in RM11-11]
Total Error: Reference source not found	1,501			+30,840 [program change]	850,680

The revisions to the cost estimates based on the requirements of this proposed rule in RM11-11 are:

- 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 and an increase of 3,840 hours, for a net increase of 3,720 annual hours. This results in $4,285,440 increase or 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 NOPR in RM11-11= $2,960,823 or $4,285,440 +$183 -$1,324,800.

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.[25] The $15.25 per entity for storage costs is an estimate based on

25 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

the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Reliability Standards.[26]

Current OMB Inventory, as approved by OMB on 9/15/2011, for ICR No. 201104-1902-001:

Number of respondents: 1,501
Average number of responses per respondent: 1
Average number of burden hours of reporting per response: 546.196
Average cost of recordkeeping per response: $3.505
Total annual burden hours: 819,840
Total annual cost burden: $5,261

FERC-725B, totals after implementation of NOPR in RM11-11Error: Reference source not found:

Number of respondents: 1,501
Average number of responses per respondent: 1
Total annual burden hours: 850,680

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

Previously reported costs, included in the current OMB-approved inventory [from ICR 201104-1902-001]:

- Reporting of $78,704,640 or $63,221,760 + $13,271,040 + $2,211,840.
- Record Retention of $5,261 for a Total Annual Cost for the FERC-725B of $78,709,901.

Cost Increase for the FERC-725B requirements contained in the NOPR in RM11-11: Total Net Annual = $2,960,823 or $4,285,440 +$183 -$1,324,800.

The total FERC-725B annual cost burden after implementation of the requirements in NOPR in RM11-11: $81,670,724 or $78,709,901 + $2,960,823.
(The total cost for the recordkeeping requirements would $5,444 (or the $5,261 from the current OMB inventory + $183 from the proposed rule in RM11-11). The $5,444 is included in the $81,670,724.)

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.[27] The $15.25 per entity for storage costs for each

---

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.
26 Based on the aggregate cost of an advanced data protection server.
27 Bureau of Labor Statistics figures were obtained from http://www.bls.gov/oes/current/naics2_22.htm, and 2009

entity is an estimate based on the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Reliability Standards.[28]

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The estimate of the cost to the Federal Government is based on salaries for professional and clerical support, as well as direct and indirect overhead costs. Direct costs include all costs directly attributable to providing this information, such as administrative costs and the cost for information technology. Indirect or overhead costs are costs incurred by an organization in support of its mission. These costs apply to activities which benefit the whole organization rather than anyone particular function or activity.

The CIP Reliability Standards do not require any information to be submitted to FERC. Neither does FERC actively verify compliance with theCIP Reliability Standards (an activity that's done by the ERO or the Regional Entities). FERC does incur costs in maintaining this collection of information current with OMB as is estimated here:

Data Clearance Program: $1,575

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

As stated in the press release available at http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=12765850,

> "[t]he Federal Energy Regulatory Commission (FERC) took steps to support continued transmission system reliability by proposing revisions to eight critical infrastructure protection reliability standards that include a new method of identifying cyber assets that are critical to the nation's bulk power grid.
>
> The proposed "Version 4" CIP standards are an interim step, FERC said in directing the electric industry and the North American Electric Reliability Corp. (NERC) to continue developing a comprehensive approach to assure the grid can withstand a cyber security incident. NERC is the Commission-certified electric reliability organization responsible for developing and enforcing mandatory reliability standards.

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.

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

The new standard would 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."

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.