Supporting Statement for

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

The Federal Energy Regulatory Commission (Commission) (FERC) requests that the Office of Management and Budget (OMB) approve **FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection**, for a three year period. FERC-725B (Control No. 1902-0248) is an existing data collection, as contained in 18 Code of Federal Regulations, Part 40.

FERC-725B pertains to standards that were previously part of a voluntary program. The Commission requests that OMB approve the estimates reported in this submission. In this submission the Commission has revised the hour and cost burden per response according to its understanding of the industry and the reporting requirements contained in this collection.

Compliance with these Reliability Standards is mandatory and enforceable for the applicable categories of entities identified in each Reliability Standard. The standards are necessary for the reliable operation of the nation's interconnected Bulk-Power System.

Background

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.[1] 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.[2]

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 standards. While NERC has developed a compliance enforcement program to ensure compliance with the reliability standards it developed, industry compliance has been voluntary and not subject to mandatory enforcement penalties. Although NERC's efforts have been important in maintaining the reliability of the nation's bulk-power system,

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

2 16 U.S.C. 824o(e)(3).

NERC itself has recognized the need for mandatory, enforceable reliability standards and has been a proponent of legislation to establish a FERC-jurisdictional ERO that would propose and enforce mandatory reliability standards.

On February 3, 2006, the Commission issued Order No. 672, implementing section 215 of the FPA.[3] Pursuant to Order No. 672, the Commission certified one organization, NERC, as the ERO.[4] 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.

RM06-22-000 NOPR

On July 20, 2007 the Commission issued a NOPR proposing to approve eight Critical Infrastructure Protection (CIP) Reliability Standards submitted by the North American Electric Reliability Corporation (NERC) for Commission approval. The CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. In addition, in accordance with section 215(d) (5) of the FPA, the Commission proposed to direct NERC to develop modifications to the CIP Reliability Standards to address specific concerns identified by the Commission. Approval of these standards will help protect the nation's Bulk-Power System against potential disruptions from cyber attacks.

On August 28, 2006, NERC submitted to the Commission for approval the following eight proposed CIP Reliability Standards:[5]

- **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification**: Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

- **CIP-003-1 – Cyber Security – Security Management Controls**: Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.

---

3 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).

4 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).

5 The Reliability Standards are not to be codified in the CFR and are not attached to the Final Rule. They are, however, available on the Commission's eLibrary document retrieval system in Docket No. RM06-22-000 and are available on the ERO's website, http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

- **CIP-004-1 – Cyber Security – Personnel & Training**:
  Requires personnel with access to critical cyber assets to have an identity verification and a criminal check. It also requires employee training.

- **CIP-005-1 – Cyber Security – Electronic Security Perimeters**:
  Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the risk-based assessment methodology required by CIP-002-1.

- **CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets**:
  Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

- **CIP-007-1 – Cyber Security – Systems Security Management**:
  Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- **CIP-008-1 – Cyber Security – Incident Reporting and Response Planning**:
  Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

- **CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets**:
  Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

NERC stated that these Reliability Standards provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks. They require Bulk-Power System users, owners, and operators to establish a risk-based vulnerability assessment methodology and use that methodology to identify and prioritize critical assets and critical cyber assets. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the responsible entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. Further, NERC explained that, because of the expanded scope of facilities and entities covered by the eight CIP Reliability Standards, and the investment in security upgrades required in many cases, NERC also developed an implementation plan that provided for a three-year phase-in to achieve full compliance with all requirements for CIP version 1 Standards.

On January 18, 2008 the Commission issued a Final Rule approving the eight Critical Infrastructure Protection (CIP) Reliability Standards submitted by the NERC for the Commission's approval. In addition, the Commission approved NERC's implementation plan that sets milestones for responsible entities to achieve full compliance with the CIP Reliability Standards. The Commission also directed NERC to develop modifications to the CIP Reliability Standards through its Reliability Standards development process to address specific concerns identified by the Commission. Similar to the Commission's approach in Order No. 693, it views such directives as a separate action from approval, consistent with the Commission's authority in section 215(d) (5) of the FPA to direct the ERO to develop a modification to a Reliability Standard.

Subsequently, on May 22, 2009, NERC filed eight "Version 2" CIP Reliability Standards, which proposed certain modifications in response to the Commission's directives set forth in Order No. 706. NERC stated that the Version 2 filing represented the result of Phase 1 of its overall plan for revising the CIP Reliability Standards to comply with Order No. 706, and that subsequent phases will address the remainder of the Commission's directives in Order No. 706. NERC also submitted two implementation plans: (1) Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2 and (2) Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards.

In an Order dated September 30, 2009, the Commission approved the Version 2 CIP Reliability Standards and directed the ERO to make certain modifications to the CIP Reliability Standards and the implementation plans within 90 days from the date of the order. The Commission directed the ERO to develop a modification to Reliability Standard CIP-006-2 to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit.[6] The Commission also directed the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6 to delete language regarding the need to remove systems from service during full operational testing. Further, the Commission found that the "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards" lacked clarity and directed NERC to submit a revised plan that clarifies certain matters.[7] The Commission rejected the "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," because it was confusing and duplicative of other documents. Finally, the Commission directed NERC to submit an update of the timetable to address the remaining Commission directives from Order No. 706.On December 29, 2010, NERC submitted a compliance filing in response to the September 30 Order. NERC explained that, while the filing proposes modifications to two CIP Reliability Standards, NERC submitted the full set of CIP Reliability Standards, CIP-002-3 through CIP-009-3, as the Version 3 CIP Reliability Standards for ease of reference and to simplify applicable entities' understanding of the appropriate implementation dates.

6 September 30 Order, 128 FERC ¶ 61,291 at P 29-30.
7 *Id*., P 41 and Attachment.

NERC modified Reliability Standard CIP-006, Requirement R1.6 to include provisions for a visitor control program:

> **R1.6** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
>
> **R1.6.1**. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
>
> **R1.6.2**. Continuous escorted access of visitors within the Physical Security Perimeter.
>
> NERC also modified Reliability Standard CIP-008-3 to remove the last sentence in Requirement R1.6, as directed by the September 30 Order.

NERC further proposed two implementation plans. First, NERC submitted an Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, revised to address the concerns and clarifications set forth in the Attachment to the September 30 Order. Second, NERC submitted an Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 (Version 3 CIP Implementation Plan), which states that prior versions of the CIP Reliability Standards will be retired when the Version 3 CIP Reliability Standards become effective. It also states that the original Version 1 Implementation Plan "is in practice retired" as of December 31, 2010.

In response to the Commission's directive, NERC included an updated timeline regarding its plans to comply with the remaining Order No. 706 directives. While not required by the September 30 Order, NERC also filed conforming changes to Violation Risk Factors and Violation Severity Levels to accommodate revisions made by the proposed Version 3 CIP Reliability Standards.[8]

On March 31, 2010, pursuant to its authority in Section 215 (d) of the FPA, the Commission issued an Order approving the modified Version 3 CIP standards, and established an effective date of October 1, 2010 for these standards.

A. Justification

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

8 The Commission does not address the Version 3 Violation Risk Factors and Violation Severity Levels submitted with this filing in this order, and will address these at a later time.

EPAct 2005 added 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 and refine the CIP standards pursuant to section 215(d) of the FPA, compliance information must be collected and/or retained to demonstrate that registered entities are protecting the physical and cyber security of the Bulk-Power System.

Recent 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 voluntary Operating Policies.[9] In response to the 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.[10] Further, the task force recommended that such legislation provide for Commission 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 was a common feature of comprehensive electricity bills since that time. A stand-alone electric reliability bill was passed by the Senate unanimously in 2000. In 2001, President Bush proposed making electric Reliability Standards mandatory and enforceable as part of the National Energy Policy.[11]

Under the new electric power reliability system enacted by the Congress (EPAct 2005, Section 215 of the FPA), the United States will 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

9 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).
10 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.
11 Report of the National Energy Policy Development Group, May 2001, at p. 7-6.

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 the improving the then-current voluntary standards and development of new Reliability Standards.[12]

Thirteen of the 46 Blackout Report Recommendations relate to cyber security. They address topics such as the development of cyber security policies and procedures; strict control of physical and electronic access to operationally sensitive equipment; assessment of cyber security risks and vulnerability at regular intervals; capability to detect wireless and remote wireline intrusion and surveillance; guidance on employee background checks; procedures to prevent or mitigate inappropriate disclosure of information; and improvement and maintenance of cyber forensic and diagnostic capabilities.[13] The CIP Reliability Standards address these and 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.[14]

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 responsible entity is not required to report to the Commission, ERO or Regional Entities, the various policies, plans, programs and procedures. However, a showing of the documented policies, plans, programs and procedures is required to demonstrate compliance with the CIP Reliability Standards.

Who uses the information?

---

12 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.

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

14 See Order No. 693 at P 234.

The responsible entity uses the information in a periodic audit in order to show compliance with the Reliability Standards.

Why is the information collected?

The purpose in documenting policies, plans, programs and procedures is to be able to show how the standard is being followed.

What are the consequences of not collecting the information?

Without this information the compliance enforcement authority would have difficulty in verifying compliance to the CIP Reliability Standards. Without verification, serious breaches in cyber security could perpetuate indefinitely before being corrected.

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 responsible entity to report anything to the Commission, ERO or Regional Entities. However, the Commission supports the use of improved technology and improved processes by responsible 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 requirements. However, all reliability requirements will be subject to FERC approval along with the 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.[15]

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 on the proposed rule on small entities. The Commission emphasizes, however, that any such limits must not weaken Bulk-Power-System reliability.

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

The Electric Reliability Organization 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, Regional Entities, and Regional Advisory Bodies annually or more frequently if so ordered by the Commission. The ERO and 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 to be prescribed by the Commission.

If the requirements under this collection were imposed less frequently the compliance enforcement authority would have difficulty in keeping up to date regarding compliance to the CIP Reliability Standards. Without current verification, serious breaches in cyber security could perpetuate before being corrected.

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.

---

15 Order No. 672 at P 330.

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 to be published in 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 rulemaking procedures also allow for public conferences to be held as required. The Commission issued a public notice on October 19, 2010 (found at http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=12465021) and received one comment from the Transmission Agency of Northern California (TANC).

Public Comment and FERC Response: TANC stated that they believed that the Commission did not adequately address or articulate the burden that falls on companies in complying with the CIP Standards and in particular, the hourly and cost burdens to comply with the documentation required by the CIP Standards. In looking at the commenter's submittal, FERC has decided to examine more carefully the burden calculations. Relying on OMB guidance in interpreting the requirements of the Paperwork Reduction Act of 1995, FERC has determined that its initial estimate of cost burden was indeed lower than is reasonable for the average respondent.

FERC maintains that the universe of respondents breaks down into three main categories: 1) Entities that have identified Critical Cyber Assets and have undergone a previous audit; 2) Entities that have not identified Critical Cyber Assets but must show compliance with CIP-003 R1 and CIP-002 R1through R3; and 3) New entities that have come into compliance with the CIP Standards and undergoing their first compliance audit. FERC's revised burden analysis is based on the average amount of time expended annually to obtain or maintain the information necessary in the event of a compliance audit. The fact that the average company may experience a spike in the burden hours immediately proceeding and during a compliance audit is accounted for in the revised estimate.

The differences between the first and third categories of respondents is that, as an entity goes through multiple compliance audits, their processes become streamlined and more automated, which then becomes reflected in a lessening of their burden. Other areas that cause the burden numbers to fluctuate deal with the size of the company, the number of overall electric assets they have, the number of critical assets and critical cyber assets that they identify, etc. Therefore, the total numbers currently used by FERC to calculate cost burden are considered the case for an average-sized company with an average number of Critical Assets and Critical Cyber Assets. It is expected that the actual burden experienced by respondents may be higher or lower than the Commission estimate, based on factors listed above.

Based on observations over several audit cycles, FERC now thinks that the preparation of the audit paperwork for an entity undergoing their first compliance audit (respondent category 3) is approximately 3840 hours. This represents 20 technical personnel working 50% of their time over 8 weeks gathering and compiling all of the required paperwork to show compliance. In addition, a secondary period that is 20% of the primary effort is estimated to be needed to respond and gather information generated from questions arising from the initial submission.

Based on observations over several audit cycles, FERC now thinks that the burden associated with ongoing compliance and preparation for future audits (respondent category 1) is less than entities coming into compliance for the first time (respondent category 3) as they are familiar with the audit compliance process and presumably will have streamlined their processes to handle the data collection effort. FERC estimates this should result in a reduction of 50% of their effort. This would result in a burden of approximately 1920 hours.

Finally, for those entities that have not identified Critical Cyber Assets but must still show compliance with CIP-003 R1 and CIP-002 R1 through R3 (respondent category 2), FERC agrees with TANC and now estimates that these entities must expend approximately 120 hours or the equivalent of 3 employees working 50% of their time for 2 weeks. FERC believes this is a reasonable estimate as the majority of these entities are small and therefore have fewer electrical assets to examine in order to determine if they have any Critical Assets, which is the first stage of the CIP-002 process.

FERC has also reconsidered dividing the burden hours by three to reflect the NERC audit schedule of 3-5 years and is instead not dividing the burden hours at all. This is due to the fact that a company will have to be obtaining and maintaining the information necessary for an audit on a consistent basis, and not only during an audit that occurs every 3-5 years. Therefore, the revised burden hours presented here represent the average annual burden hours per respondent, including the spikes that may result during an audit.

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 filed to be confidential. However, certain 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 cyber security 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

Current OMB Inventory:

The average burden hours per response reflect the time necessary to implement the initial CIP reliability standards. Ongoing compliance burden was not estimated at the time the collection was first approved.

Number of respondents: 1000
Average number of responses per respondent: 1
Average number of burden hours per response: 1125.4
Total annual burden hours: 1,125,400

Proposed Estimate from October Public Notice

The extent of the reporting burden is influenced by the number of identified critical assets and related critical cyber assets pursuant to CIP-002. An entity identifying one or more critical cyber assets, including assets located at remote locations, will likely require more resources to demonstrate compliance with the CIP Reliability Standards compared to an entity that identifies no critical assets. The Commission has developed estimates using data from NERC's compliance registry as well as a 2009 survey that was conducted by NERC to asses the number of entities reporting Critical Cyber Assets. The updated annual estimates follow.

Data Collection	No. of Respondents[16]	Average No. of Responses Per	Average No. of Burden Hours	Total Annual Hours

16 The NERC Compliance Registry as of 9/28/2010 indicated that 2079 entities were registered for NERC's

	(1)	Respondent (2)	Per Response[17] (3)	(1)x(2)x(3)
FERC-725B				
Estimate of U.S. Entities that have identified Critical Cyber Assets	345	1	320	110,400
Estimate of U.S. Entities that have not identified Critical Cyber Assets	1,156	1	8	9,248
New U.S. Entities that have to come into compliance with the CIP Standards[18]	6*	1	1,176	7,056
Totals	1,501 Error: Reference source not found			126,704

*not included in the 1,501 total because it is assumed that on average, six entities per year will no longer have to comply with the CIP standards, offsetting the additional 6 entities.

Revised Estimate in Response to Comment and Further Analysis

compliance program. Of these, 2057 were identified as being U.S. entities. Staff concluded that of the 2057 U.S. entities, only 1501 were registered for at least one CIP related function. According to an April 7, 2009 memo to industry, NERC's VP and Chief Security officer noted that only 31% of entities responded to an earlier survey and reported that they had at least one Critical Asset, and only 23% reported having a Critical Cyber Asset. Staff applied the 23% reporting to the 1501 figure to obtain an estimate of the number of entities that have identified Critical Cyber Assets. The 6 new entities listed here are assumed to match a similar set of 6 entities that would drop out in an existing year. Thus, the net estimate of respondents remains at 1501 per year.

17 This figure relates to NERC's audit schedule which requires NERC to engage in a compliance Audit once every 3 to 5 years. For simplicity, staff has divided the total number of hours by 3 to reflect the amount of time annually spent preparing documents. Staff assumed that each CIP audit or spot check would require four individuals 6 weeks to prepare and demonstrate compliance with CIP standards for entities that have identified Critical Cyber Assets. Staff estimated that entities that do not have Critical Cyber Assets would still be required to demonstrate compliance with CIP-002, which would require one individual approximately three days to execute.

18 This category of respondents (with the corresponding burden) was not included in the 60-day public notice due to an oversight by Commission staff.

The revised estimated annual burden is shown below in accordance with the discussion above. The Commission has developed estimates using data from NERC's compliance registry as well as a 2009 survey that was conducted by NERC to asses the number of entities reporting Critical Cyber Assets.

Data Collection	No. of Respondents[19] (1)	Average No. of Responses Per Respondent (2)	Average No. of Burden Hours Per Response[20] (3)	Total Annual Hours (1)x(2)x(3)
FERC-725B				
Category 1 - Estimate of U.S. Entities that have identified Critical Cyber Assets	345	1	1,920	662,400
Category 2 - Estimate of U.S. Entities that have not identified Critical Cyber Assets	1,156	1	120	138,720
Category 3 - New U.S. Entities that have to come into compliance with the CIP Standards[21]	6	1	3,840	23,040

19 The NERC Compliance Registry as of 9/28/2010 indicated that 2079 entities were registered for NERC's compliance program. Of these, 2057 were identified as being U.S. entities. Staff concluded that of the 2057 U.S. entities, only 1501 were registered for at least one CIP-related function. According to an April 7, 2009, memo to industry, NERC's VP and Chief Security officer noted that only 31% of entities responded to an earlier survey and reported that they had at least one Critical Asset, and only 23% reported having a Critical Cyber Asset. Staff applied the 23% reporting to the 1501 figure to obtain an estimate of the number of entities that have identified Critical Cyber Assets. The 6 new entities listed here are assumed to match a similar set of 6 entities that would drop out in an existing year. Thus, the net estimate of respondents remains at 1501 per year.

20 Calculations:

Respondent category 3:

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

Respondent category 2:

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

Respondent category 1: 50% of 3840 hours = 1920

Entities no longer required to comply with CIP Standards (Two category 1 respondents and four category 2 respondents)	Category 1: - 2	1	Category 1 (2 respondents) : 1,920	- 3,840
	Category 2: - 4		Category 2 (4 respondents) : 120	- 480
Totals	1,501			819,840

Summary of Changes

FERC-725B	**Current OMB Inventory**	**Proposed New OMB Inventory**
Estimated number of respondents	1,000	1,501
Estimated number of responses per respondent	1	1
Estimated number of responses per year	1,000	1,501
Estimated number of hours per response	1,125.4	546.196
Total estimated burden (hours per year)	1,125,400	819,840
Program change in industry burden hours		0
Adjustment change in industry burden hours		-305,560
Net Change in Hours[22]		**-305,560**

21 These respondents and those in the subsequent column of the table (with the corresponding burden and cost figures) were not included in the 60-day public notice due to an oversight by Commission staff.

22 The change is due to two factors. First, existing entities in the industry should now be fully compliant with the CIP initial standards, and therefore (all but a few companies), should be incurring a much reduced ongoing burden:
1000 responses X (1125.4 hours per response – 546.196 hours per response) = 579,204 hours of reduction.
Second, 501 additional entities are included in the revised estimate and have the ongoing burden:
501 responses X 546.196 hours per response = 273,644 hours of increase.
The net change is a reduction of 305,560 hours.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

Previously reported costs:

The Commission previously reported $24,758,800 per year until implementation was fully completed (in 2010). Ongoing costs were not calculated at that time.

Revised cost estimates based on the revised burden estimates above:

- Category 1, Entities that have identified Critical Cyber Assets = 658,560 (662,400-3,840) hours@$96/hour = $63,221,760
- Category 2, Entities that have not identified Critical Cyber Assets = 138,240 (138,720-480) hours@$96/hour = $13,271,040
- Category 3, New U.S. Entities that have to comply with CIP Standards = 23,040 hours@$96/hour = $2,211,840
- Storage Costs for Entities that have identified Critical Cyber Assets[23] = 345 Entities@$15.25/entity = $5,261
- **Total Annual Cost for the FERC-725B = $78,709,901**

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.[24] The $15.25 per entity for storage costs for each entity is an estimate based on the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Standards.[25]

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.

---

23 This cost category was not included in the 60-day public notice due to an oversight by Commission staff.
24 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.
25 Based on the aggregate cost of an IBM advanced data protection server.

The standards do not require any information to be submitted to the Commission, neither does the Commission actively verify compliance with these standards (this is done by the ERO or Regional Entities). The Commission 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

The adjustment decrease of 305,560 hours is due to two factors. The first is that the multi-year implementation period for these initial CIP standards was completed in 2010 (a reduction of 579,204 hours). It is now assumed that most entities (all but an average of 6 new entities per year) are incurring the much reduced burden requisite with demonstrating ongoing compliance as opposed to initial implementation. The second factor is an increase in the number of applicable entities which is due to a more accurate estimate of the effected industry (an increase of 273,644 hours). The net burden change is a reduction of 305,560 hours.Error: Reference source not found

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 data that is created or maintained as part of this publication.

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 Reliability Standard.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS.

This is not a collection of information employing statistical methods.