

Supporting Statement

FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection
(As modified in the NOPR in Docket No. RM13-5, issued 4/18/2013)

FERC is resubmitting this proposed rule for administrative purposes only. The original submission was decided on by OMB on 7/16/2013 (ICR #201304-1902-001).

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. RM13-5.¹ FERC-725B (OMB Control No. 1902-0248) is an existing data collection, as contained in 18 Code of Federal Regulations (CFR), Part 40.

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, The Electricity Modernization Act of 2005, which is Title XII of the Energy Policy Act of 2005 (EPAAct 2005), was enacted into law.² EPAAct 2005 added a new section 215 to the Federal Power Act (FPA), which requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved the Reliability Standards may be enforced by the ERO, subject to Commission oversight.

On January 18, 2008, the Commission issued Order No. 706, which approved the CIP version 1 Standards to address cyber security of the Bulk-Power System.³ In Order No. 706, the Commission approved eight CIP Reliability Standards (CIP-002-1 through CIP-009-1). While approving the CIP version 1 Standards, the Commission also directed NERC to develop modifications to the CIP version 1 Standards, intended to enhance the protection provided by the CIP Reliability Standards. Subsequently, NERC filed the CIP version 2 and CIP version 3 Standards in partial compliance with Order No. 706. The Commission approved these standards in September 2009⁴ and March 2010,⁵ respectively.

1 The Commission also issued an errata notice (at <http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=13252411>) in this docket on 5/3/2013 correcting a few mistakes in the proposed rule.

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

3 *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), *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

4 *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009).

5 *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010).

On April 19, 2012, the Commission issued Order No. 761, which approved the CIP version 4 Standards (CIP-002-4 through CIP-009-4).⁶ Reliability Standard CIP-002-4 (Critical Cyber Asset Identification) sets forth 17 uniform “bright line” criteria for identifying Critical Assets. The Commission also accepted NERC’s proposed implementation schedule for the CIP version 4 Standards, which are scheduled for full implementation and enforceability beginning April 2014.⁷

In its petition to the Commission to approve the CIP version 5 standards, NERC states that it took into consideration 4 years of experience since the first CIP standards were implemented, “as well as FERC directives...developed the proposed CIP Version 5 standards to better protect the reliability of the nation’s Bulk Electric System (“BES”) from cyber-attacks.”⁸

NERC goes on to state that:

The improvements included in CIP Version 5 reflect a maturity of the NERC CIP program. While the general framework of the proposed standards follow the organization of the previous CIP versions, a new process is introduced in proposed CIP-002-05 for identifying and classifying BES Cyber Systems according to “Low-Medium-High” impact. Once BES Cyber Systems are identified, a Responsible Entity must then comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria relating to impact and other characteristics such as communications connectivity. As such, NERC and its stakeholders have proposed the most comprehensive set of mandatory cybersecurity standards ever utilized on a widespread basis in the electric industry.

In terms of information collection, the CIP standards require entities to document their compliance with requirements and to develop cyber security policies and procedures.

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

The information collection requirements in the CIP Version 5 standards apply to entities registered as the following functions: balancing authorities, distribution providers, generator operators, generator owners, interchange coordinators (or interchange authorities), reliability

⁶ *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 Fed. Reg. 24,594 (April 25, 2012), 139 FERC ¶ 61,058 (2012); *order denying reh’g*, 140 FERC ¶ 61,109 (2012).

⁷ The CIP version 5 Implementation Plan, if approved as proposed in the NOPR, would obviate this CIP version 4 schedule.

⁸ The NERC Petition is available on FERC’s eLibrary system (<http://www.ferc.gov/docs-filing/elibrary.asp>) by searching in Docket Number RM13-5. The proposed standards are contained in Exhibit A of NERC’s petition.

coordinators, transmission operators, and transmission owners. Based on the NERC compliance registry, FERC estimates there are 1,475 entities registered for at least one of the functions listed above. Each of these entities are considered “respondents” for the purposes of fulfilling the paperwork requirements.

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

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

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

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

4. DESCRIBE EFFORTS TO IDENTIFY DUPLICATION AND SHOW SPECIFICALLY WHY ANY SIMILAR INFORMATION ALREADY AVAILABLE CANNOT BE USED OR MODIFIED FOR USE FOR THE PURPOSE(S) DESCRIBED IN INSTRUCTION NO. 2

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

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

The CIP Version 5 Reliability Standards generally do apply to small entities, depending first on their registered function(s) and then on the type of facilities they own. Nearly all of the small entities, which are subject to the CIP version 5 standards, own *only* facilities that should fall into the Low impact category for these standards. This means the burden for these entities is relatively minor compared with the rest of the applicable entities. The CIP Version 5 Reliability Standards only require owners of Low impact category facilities to create and implement policies⁹ to protect their cyber assets. The Requirements for Low impact category facilities do not impose any specific, technical security controls, which will provide small entities with more flexibility in complying with the standards. As FERC stated in Order No. 761, "...control systems that support Bulk-Power System reliability are only as secure as their weakest links, and that a single vulnerability opens the computer network and all other networks with which it is interconnected to potential malicious activity."¹⁰ Due to the inherent connectivity between entities that must occur to operate the Bulk-Power System, the CIP Version 5 Reliability Standards cannot exclude entities based on size alone without creating a weak point in the security of the Bulk-Power System that can be exploited to navigate to higher value cyber systems.

The Standard Drafting Team considered the impact on small entities when setting the cyber asset impact classification levels and intended that the Low cyber assets would be provided with the least effort and cost, compared to other impact levels.

The Commission estimates the NOPR will impact 536 small entities.¹¹ Of this amount, the Commission estimates that only 14 small entities¹² (2.6 percent of the total number of small entities) may, on average, experience a significant economic impact of \$116,000 per entity in the first year, \$145,000 in the second year, and \$88,000 in the third year.¹³ This cost is primarily due

⁹ CIP-003-5 Requirement R2 specifies 4 policies that apply to Low Impact Systems: 1) Cyber security awareness; 2) Physical security controls; 3) Electronic access controls; 4) Incident response to a cyber-security incident.

¹⁰ *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 FR 24594 (Apr. 25, 2012), 139 FERC ¶ 61,058 (2012) *order denying reh'g*, 140 FERC ¶ 61,109 (2012), Paragraph 80.

¹¹ Based on a comparison of the NERC Compliance Registry (as of February 28, 2013) and Energy Information Administration Form 861 (*available at* <http://www.eia.gov/electricity/data/eia861/index.html>)

¹² The 14 small entities in this class represent small Transmission Owners assumed to fall under the Medium classification and thus experience a greater impact than other small entities. These same entities also experience the impact associated with the Low classification.

¹³ These costs are based on an estimated 4,600 hours of total work per entity over three years at \$59/hour and \$15,000 of non-labor costs.

to implementation during the compliance period. After the initial implementation the Commission expects the average annual cost per each of the 14 entities to be less than \$64,000. The Commission has determined that 2.6 percent of the effected small entities do not represent a “substantial number” in terms of the total number of regulated small entities applicable to the NOPR.

The Commission estimates that 234 out of the 536 small entities¹⁴ will each experience an average economic impact of \$29,000 per year during years two and three.¹⁵ Finally, the Commission estimates that the remaining 288 out of the 536 small entities¹⁶ will only experience a minimal economic impact.

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

As stated in response to item #2, the documentation related to the CIP reliability standards is an integral part of maintaining cyber security. The power grid would be at greater risk to cyber threats if the collection was conducted less frequently.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

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

Entities may have to submit to or show the auditors security or confidential information that is related to the CIP standards. The general practice is that the auditor returns the confidential information to the entity following the audit.

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

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

The ERO process to establish Reliability Standards is a collaborative process with the ERO, Regional Entities and other stakeholders developing and reviewing drafts, and providing

¹⁴ This figure represents the number of small entities that own assets covered by CIP version 5. This number does not include the 14 significantly impacted entities.

¹⁵ This cost figure is based on an estimated 268 hours of total work per entity for each of years two and three combined at \$72/hour, and \$7,500 of non-labor costs for each of years two and three.

¹⁶ The number of small Distribution Providers assumed to not own assets covered by CIP version 5.

comments, with the final proposed standard submitted to the FERC for review and approval.¹⁷ In addition, each FERC rulemaking (both proposed and final rules) is published in the Federal Register, thereby providing public utilities and licensees, state commissions, Federal agencies, and other interested parties an opportunity to submit data, views, comments or suggestions concerning the proposed collection of data. The proposed rule was published in the Federal Register on April 24, 2013 (78 FR 24107). The Commission also issued an errata notice¹ in this docket on May 5, 2013 correcting a few mistakes in the proposed rule.

In the NOPR the Commission proposes to approve the CIP version 5 Standards as an improvement over the currently –approved CIP Reliability Standards. However, certain aspects of the proposed standards raise concerns regarding the potential ambiguity and, ultimately, the enforceability of the CIP version 5 Standards. For a summary of the Commission’s concerns and requests for comment, see the paragraphs 4-10 of the proposed rule.¹⁸

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

There are no payments or gifts for respondents related to this collection.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

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

11. PROVIDE ADDITIONAL JUSTIFICATION FOR ANY QUESTIONS OF A SENSITIVE NATURE

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

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

The Commission based its paperwork burden estimates on the difference between the latest Commission-approved (and OMB approved for the information collection requirements) version of the CIP Reliability Standards (CIP version 4) and the estimated paperwork burden resulting from CIP version 5 Reliability Standards (CIP Version 5).

¹⁷ Details of the current ERO standard processes are available on the NERC website at http://www.nerc.com/docs/standards/sar/Appendix_3A_Standard_Processes_Manual_20100903_2_.pdf.

¹⁸ The proposed rule is included as a supplementary document in ROCIS/Reginfo.gov.

The paperwork burden under CIP version 5 is different than that imposed by CIP version 4. Under CIP version 4, all applicable entities must first identify, by applying criteria specified in CIP-002-4, which of the Cyber Assets they own are subject to the mandatory protections specified in the remaining CIP standards. Those identified Cyber Assets are termed Critical Cyber Assets (CCA) in CIP version 4. If, upon completion of the required process in CIP-002-4, the entity has identified at least one CCA, it must implement all mandatory protections specified in the remaining CIP Reliability Standards with respect to any identified CCA. If, on the other hand, the entity determines that it does not own any CCAs, it is not required to implement any of the protections specified in the remaining CIP version 4 Standards.

By contrast, CIP version 5 does not use the term CCA. Under CIP version 5, a responsible entity identifies Cyber Assets for protection by applying the CIP-002-5 definitions and classification criteria. The responsible entity is required to comply with at least some mandatory protections in the remaining standards for all Cyber Assets identified as BES Cyber Systems. The specific mandatory protections with which the responsible entity must comply depends on whether the the Cyber Assets it owns and identifies as BES Cyber Systems are classified as Low, Medium, or High impact by CIP-002-5 Attachment 1 (and other characteristics detailed in various individual requirements). Each responsible entity that owns Cyber Assets identified as BES Cyber Systems will be concerned at least with the Low impact classification.

Because the change in paperwork burden between CIP version 4 and CIP version 5 differs depending upon the extent to which that entity had to comply with CIP version 4, we delineate the registered entities into three groupings related to their status under CIP version 4, as follows:

- **Group A:** Entities that are not subject to the CIP version 4 Standards, but are subject to the CIP version 5 Standards. The Group A entities consist of those Distribution Providers that are not also registered for another CIP function, such as the Load Serving Entity function (which is subject to CIP version 4). All of these entities are concerned only with the Low classification because they do not own any assets classified as Medium or High under CIP-002-5 Attachment 1.
- **Group B:** Entities that are registered for functions subject to CIP version 4, but that did not identify any CCAs under CIP-002-4. Therefore, Group B entities do not own facilities that require the implementation of mandatory protections specified by the remaining CIP version 4 Standards. Cyber Assets that would not have been subject to mandatory protections under the CIP version 4 Standards are not classified as High impact under the CIP version 5 Standards. Therefore, Group B entities do not own any assets classified as High impact by CIP-002-5 Attachment 1, and are concerned with only

the Low and potentially Medium impact classifications (depending whether any assets they own meet the Medium criteria).

- **Group C:** Entities that are registered for functions subject to CIP version 4 *and* that identify, upon completion of the CIP-002-4 analysis, at least one asset as a CCA. Therefore, Group C entities own facilities that require the implementation of the mandatory protections specified in the remaining CIP version 4 Standards. Most types of Cyber Assets that would be subject to mandatory protections under the CIP version 4 Standards (all except blackstart generation and cranking path facilities) are classified as either High or Medium impact under the CIP version 5 Standards. Therefore, Group C entities potentially own Cyber Assets that are classified as High or Medium impact by CIP-002-5 Attachment 1, and are concerned with all three impact classifications (depending on the extent to which the assets they own meet the Medium or High criteria).

NERC states on its website that, “All bulk power system owners, operators, and users must comply with approved NERC Reliability standards. These entities are required to register with NERC through the appropriate regional entity.”¹⁹ The NERC Compliance Registry as of February 28, 2013 indicated that 1,927 entities were registered for NERC’s compliance program. Of these, 1,911 were identified as being U.S. entities. Staff concluded that approximately 1,475 U.S. entities were registered for at least one CIP-applicable function, and therefore must comply with the proposed CIP version 5 Reliability Standards. Further, 1,414 are subject to the currently approved CIP version 4. There is one functional registration that was not subject to CIP version 4 (or other prior versions) but which is now subject to CIP version 5, by virtue of being added to the list of responsible entities under the Applicability section of each of the CIP version 5 Standards (Distribution Providers). However, many entities registered for the Distribution Provider function are also registered for another function that made them subject to CIP version 4 (and past versions). The net difference (the entities registered such that they are subject to CIP version 5 but are not subject to CIP version 4) are the entities that constitute Group A (61 entities).

Consistent with the Commission’s approach in Order No. 761 (CIP version 4),²⁰ we assume that 23 percent (325 unique entities) of the 1,414 US entities subject to CIP version 4 identified CCAs (Group C). It follows that the remaining 77 percent (1089 unique entities) of the U.S. entities did not identify any CCAs under CIP version 4 (Group B). This ratio factors into several of the calculations needed to estimate the differences in effort among entities in Group B, as compared to Group C.

To estimate the change in paperwork burden between CIP version 4 and proposed CIP version 5, we recognize that the entities in all groups will undertake the following paperwork tasks to at

¹⁹ See the “Who Must Comply?” section at <http://www.nerc.com/pa/comp/Pages/Default.aspx>.

²⁰ See Order No. 761, 139 FERC ¶ 61,058 at P 122, n.162.

least some extent: 1) create or modify documentation of processes used to identify and classify the cyber assets to be protected under the CIP Reliability Standards; 2) create or modify policy, process and compliance documentation; and 3) create and maintain documentation related to compliance activities. Entities have two years to comply with requirements applicable to Cyber Assets classified as High or Medium, and three years to comply with requirements applicable to those classified as Low. We assume that entities with High or Medium assets will incur burden over years one and two and entities with Low assets will incur burden over years two and three.

We estimate the level of paperwork burden for each Group as follows:

- No more than 10 percent of the Group A entities, and all of Group B & C entities will own at least one subject facility classified as Low under the CIP version 5 Standards. We estimate 24 hours²¹ per entity to develop its evaluation process documentation for identifying the facilities subject to the standard, and 1,024 hours²² to develop the required documentation for covered assets. We divide the total burden hours between the second and third years of the compliance period allowed for the facilities classified as Low because this is when we assume the entities will do the work.
- The burden hours for facilities classified as Medium and High are split between the first and second year, since Groups B and C are allowed a 24-month period to bring them into compliance. (The third year figure shown for these rows represents an ongoing effort level). Except for Group C Blackstart facilities (see bullet on Blackstart facilities below), we assume 32 hours²³ per entity for development of its evaluation process documentation.
- We assume no more than 30 percent of Group B and Group C entities will own one or more of the newly covered transmission facilities classified as Medium. For those Group B entities that do, we assume 3,200 hours²⁴ to develop the required policy, compliance and implementation documentation for the 10 standards, and 832 hours²⁵ per entity for ongoing compliance burden. For those Group C²⁶ entities that do, we assume 832 hours²⁷ per entity for ongoing compliance burden.

21 Based on assumption of 2 persons per entity, working 15 percent of the time for 2 weeks.

22 Based on assumption of 2 persons per entity, creating required policy documentation per policy (for each of four low policies), working 40 percent of the time for 8 weeks.

23 Based on assumption of 2 persons per entity, working 20% of the time for 2 weeks.

24 Based on assumption of 1 person per entity, per standard (for each of the 10 standards) creating policy documentation, working 75 percent of the time for 8 weeks, and 1 person per entity, per standard (for each of the 10 standards) on creating compliance documentation, 25 percent of the time for 8 weeks. Therefore, for the estimated 10 standards per entity, 1 person would be working 3,200 hrs.

25 Based on assumption of 2 persons per entity, working 20 percent of the time for 52 weeks.

26 These are the Group C Medium facilities that are newly applicable to CIP standards. The total number of entities is 23 (30% of 78 new Mediums = 23).

27 Based on assumption of 2 persons per entity, working 20 percent of the time for 52 weeks.

- With respect to the Blackstart facilities owned by Group C entities, we assume 160 hours²⁸ per entity to modify policy and evaluation process documentation. We also assume a *reduction* of 728 hours²⁹ per entity for ongoing compliance documentation that is required under the currently approved CIP standards but is no longer required under CIP version 5.
- For Group C’s Medium and High facilities, we assume 1,600 hours³⁰ per entity to modify the required policy, compliance, and implementation documentation, and 416 hours³¹ per entity for ongoing compliance.

The estimated paperwork burden changes for these entities, as contained in the proposed rule in RM13-5-000, are illustrated in the table below. The information collection burden also varies according to the types of facilities the entities own, as classified by the criteria in CIP-002-5, Attachment 1. To further refine our estimate, we indicate the classes of facilities each group of entities owns in the second column of the table below.

Groups of Registered Entities	Classes of Entity’s Facilities Requiring CIP Version 5 Protections	Number of Entities³²	Total Hours in Year 1 (hours)³³	Total Hours in Year 2 (hours)	Total Hours in Year 3 (hours)
Group A	Low ³⁴	61	0	3,804	3,804
Group B	Low ³⁵	1,089	0	570,636	570,636

28 Based on assumption of 1 person per entity, per standard (for each of the 10 standards) modifying policy documentation, working 10 percent of the time for 2 weeks, and 1 person per entity, per standard (for each of the 10 standards) modifying compliance documentation, 10 percent of the time for 2 weeks.

29 Based on assumption of a *reduction* of 2 persons per entity, collecting compliance data, working 20 percent of the time for 52 weeks (giving a reduction of 832 hours), and an *increase* of 1 person per entity, collecting compliance data, working 5 percent of the time for 52 weeks (giving an increase of 104 hours), for a net reduction of 728 hours. CIP v5 puts Blackstart facilities into the Low category. This reduces the amount of paperwork burden these facilities have under the current CIP standards.

30 Based on assumption of 1 person per entity, per standard (for each of the 10 standards) modifying compliance documentation, working 50 percent of the time for 8 weeks.

31 Based on assumption of 2 persons collecting compliance data, working 10 percent of the time for 52 weeks.

32 Group A includes 61 unique entities, Group B includes 1,089 unique entities, and Group C includes 325 unique entities.

33 The three “Total Hours” columns represent the aggregate hours for all the entities in each row. For the last row they show the grand total for each year.

34 Distribution Providers are the only functional entity type in Group A (*see* section 4, Applicability, of each CIP version 5 Standard), and their facilities are captured only by the Low classification criteria listed in proposed CIP-002-5. The number of entities in this group represents the number of Distribution Providers that are not registered for any additional CIP version 5 applicable functions, including the Load Serving Entity function. The Load Serving Entity function is subject to CIP versions 1-4.

35 As with Groups A and C, Group B will own Low facilities which were not identified for protections

Group B	Medium ³⁶	260	128,960	128,960	64,896
Group C	Low ³⁷	325	0	170,300	170,300
Group C	Medium (New) ³⁸	78	1,248	1,248	19,136
Group C	Low ³⁹ (Blackstart)	283	22,640	22,640	-206,024
Group C	Medium or High ⁴⁰	325	265,200	265,200	135,200
Totals⁴¹			418,048	1,162,788	757,948

The following shows the average annual cost burden (averaged over Years 1-3 and rounded for hours/entity) for all entities within the group, based on the burden hours in the table above:⁴²

- Group A: 61 unique entities * 41.5 hrs/entity * \$72/hour = \$182,000
- Group B: 1,089 unique entities * 448 hrs/entity * \$72/hour = \$35,127,000
- Group C: 325 unique entities * 889 hrs/entity * \$72/hour = \$20,803,000

under prior CIP versions. The number of Group B respondents is calculated as 77 percent of the total entities previously subject to the CIP Reliability Standards. (0.77 * 1414 = 1,089).

36 In contrast to CIP version 4, Criterion 2.5 in proposed CIP version 5 identifies new facilities for protection (transmission facilities which are greater than or equal to 200kV and less than 300kV) and classifies them as “Medium.” Some of these newly-applicable transmission facilities are owned by entities that had not previously identified any CCAs under previous versions, while some of the Criterion 2.5 facilities are owned by entities that previously identified CCAs. Assuming Group B entities constitute 77 percent of the entities to which this criterion potentially applies, 260 entities of the 338 total Transmission Owners (TO) captured by Criterion 2.5 are assigned to Group B, while the remaining 78 are allotted to Group C.

37 As with Groups A and B, the entities that identified CCAs under CIP version 4 (Group C) will also own facilities newly addressed by CIP version 5 and classified as Low. The number of Group C respondents is calculated as 23 percent of the total entities previously subject to the CIP Reliability Standards. (0.23 * 1414 = 325).

38 This row concerns only the newly subject transmission facilities that are addressed by CIP version 5, Criterion 2.5, as owned by Group C TO (Transmission Owner) entities. See the Footnote 25 for Group B Medium for further explanation. These Medium-rated facilities are broken out in this row, separate from other Medium facilities the entity may own in the High and Medium rows below because the level of effort for these Group C TO entities to protect these newly protected facilities is estimated differently than for the Group B entities, or for other Medium facilities the entity may own.

39 Blackstart generation and transmission cranking paths are the only types of facilities identified first for more specified security controls under CIP version 4, Criteria 1.4 and 1.5, but then subject only to Low mandatory security controls under CIP version 5, Criterion 3.4. The number of entities in this row represents 23 percent of the sum of all registered Generation Operators (891 total Generator Operators) to account for Blackstart Resources and all TOs to account for cranking paths. The total burden in year 3 is negative (-206,024 hours) because in year 3 blackstart facilities will no longer be subject to the more specified security controls under CIP version 4. This leads to the burden reduction for these entities described in footnote 17.

40 Except for the Blackstart facilities noted above, the facilities that Group C entities identify as CCAs under CIP version 4 will be rated for Medium or High security controls under CIP version 5.

41 In the NOPR, the total for year 2 and the total for year 3 were shown to be 768 hours more than the actual totals. The Commission is issued an errata notice on 5/3/2013 to correct the error.

42 The total cost figures are rounded to the nearest thousand dollars. The “hours per entity” figures are averages over three years. Some entities within a group may experience higher or lower hourly impact (as illustrated in the burden table) depending on entity type and assets owned.

Total average annual paperwork cost (averaged over Years 1-3) for the change in requirements contained in the NOPR in RM13-5 = \$56,112,000. [(\$182,000 + \$35,127,000 + \$20,803,000) = \$56,112,000].

The estimated hourly rate of \$72 is the average loaded cost (wage plus benefits) of legal services (\$128.00 per hour), technical employees (\$58.86 per hour) and administrative support (\$30.18 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics.⁴³ The existing burden hours for FERC-725B are 850,680. In this clearance package we request a 286,927 hour downward adjustment, and a 779,595 hour program increase, as explained in item #15.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

The main potential non-labor cost is for electronic record storage. The Commission considers any cost related to storing CIP standard documents to be negligible. However, the Commission will continue with the current records storage cost of \$15.25 per entity per year for each of the applicable entities (331 total (331*\$15.25=\$5,047 (rounded down))).⁴⁴

There are no other non-labor costs associated with the CIP version 5 standards.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The CIP Reliability Standards do not require any information to be submitted to FERC. Most of the FERC cost 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 indicated in the following table.

FERC-725B Federal Cost	Estimated Annual Federal Cost ⁴⁵
PRA Administration Cost ⁴⁶	\$2,250

43 See http://bls.gov/oes/current/naics2_22.htm and <http://www.bls.gov/news.release/ecec.nr0.htm>.

44 These are the entities that had identified critical cyber assets under CIP Version 3 and 4. For version 3 and version 4 there were 345 of these entities. Now, there are 325, plus an additional 6 entities brought in by version 5, for a total of 331 entities incurring this recordkeeping cost. We assume that all other entities will experience negligible record keeping costs.

45 Based on 2013 cost per FTE of \$145,818.

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

FERC has issued a proposed rule which proposes to adopt the CIP version 5 Reliability Standards. As discussed previously, these standards are an improvement over the current Version 4 standards. The CIP version 5 standards will require new and ongoing paperwork burden.

FERC is averaging the estimated burden hours from the proposed rule across the first three years to create an annual figure to provide to OMB. This annual figure is 779,595 hrs [(418,048 hrs + 1,162,788 hrs + 757,948 hrs)/3 = 779,595 hrs]. After the first three years, entities will have completed implementation of CIP version 5 and the total burden will be reduced by 383,543 hours/year.⁴⁷

FERC proposes to add the annual hours from the NOPR, 779,595 hours, to an adjusted baseline of burden hours under the existing CIP standards. The current burden inventory shows 850,680 hours. FERC is adjusting the existing hours based upon careful review of the assumptions used to generate the previous estimates.

- In particular, one of the assumptions was that entities would incur the full burden of preparing for an audit *each year* instead of every 3-5 years. A small fraction of entities may be responsible for multiple functions and be audited on a more frequent basis but this is the exception and not the rule. We account for that in the adjusted figure. The total burden reduction for modifying this assumption is 429,600 hours.
- Also, the assumptions did not include some of the yearly burden required to keep documents up to date for future audits. The change here leads to a 143,208 hour increase.
- Finally, there are an estimated net 26 fewer entities now than there were the last time OMB approved this collection (a reduction from 1,501 to 1,475). This change leads to a 534 hour burden reduction. CIP version 5 adds 61 entities leading to an overall change of -26 entities. The general reason for the reduction in entities is caused by some entities merging and some entities dropping from the market.

⁴⁶ The PRA Administration Cost is based on the Commission's estimated staff time and resources to comply with the requirements of the PRA.

⁴⁷ This figure represents the burden hours associated with implementing the CIP version 5 standards. The remaining hours are associated with the ongoing burden.

The total change due to agency adjustment is 286,927 hours⁴⁸ (143,208 hours – 429,600 hours – 534 hours = 286,927 hours). See the spreadsheet attached to this package for more details regarding this agency adjustment change.

FERC does not consider there to be any additional non-labor costs for CIP version 5. The adjustment (-\$397) in the annual cost burden below is due to fewer applicable entities (going from 357 entities to 331 entities estimated to incur this cost).

This table shows the adjustments and discretionary changes to the burden estimates, as described previously.

FERC-725B	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	1,475	1,501	-87	61
Annual Time Burden (Hr)	1,343,348	850,680	-286,927	779,595
Annual Cost Burden (\$)	5,047	5,444	-397	0

16. TIME SCHEDULE FOR PUBLICATION OF DATA

There are no publications of data as part of this collection.

17. DISPLAY OF EXPIRATION DATE

It is not appropriate to display the expiration date because the information is not collected on a preformatted form or in any format that would allow for such a display.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

The Commission does not use statistical methods for this collection.

⁴⁸ The math show here actually yields 286,926 hours. However, in ROCIS the adjustment is rounded to 286,927 hours.