FERC-725B2 (OMB Control No. 1902-0304)
Docket No. RD21-2-000
(CLO issued March 18, 2021)

Supporting Statement for
FERC-725B2 (Mandatory Reliability Standards, Critical Infrastructure Protection (CIP)), as modified in Docket No. RD21-2-000)

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review and approve for three years FERC-725B2 (Mandatory Reliability Standards, Critical Infrastructure Protection (CIP)) as modified in Docket No. RD21-2-000.

1. CIRCUMSTANCES THAT MAKE THE COLLECTION OF INFORMATION NECESSARY

On August 8, 2005, the Electricity Modernization Act of 2005, which is Title XII of the Energy Policy Act of 2005 (EPAct 2005), was enacted into law. EPAct 2005 added a new Section 215[1] 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. In 2006, the Commission certified the North American Electric Reliability Corporation (NERC) as the ERO pursuant to FPA section 215.[2]

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. 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 2009 and March 2010, respectively.

In Order No. 850, the Commission approved Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 (the "Supply Chain Standards"). The Supply Chain Standards, which were developed in response to Order No. 829, address cybersecurity risks associated with the supply chain for BES [Bulk Electric System] Cyber Systems.[3] In approving the Supply Chain Standards, the Commission found that they addressed the following four objectives from Order No. 829:

(1) software integrity and authenticity;

---

1 16 U.S.C. 824*o*.
2 *North American Electric Reliability Corp.*, 116 FERC 61,062, *order on reh'g & compliance*, 117 FERC 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).
3 Revised Critical Infrastructure Protection Reliability Standards, Order No. 829, 156 FERC 61,050 (2016) [hereinafter Order No. 829].

(2) vendor remote access protections;
(3) information system planning; and
(4) vendor risk management and procurement controls.[4]

While approving the Supply Chain Standards, the Commission determined that a significant cybersecurity risk associated with the supply chain for BES Cyber Systems remained because the approved Reliability Standards did not address Electronic Access Control or Monitoring Systems (EACMS).[5] To address this reliability gap, pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directed NERC to develop and submit modifications to include EACMS in the supply chain risk management Reliability Standards and to file the modifications within 24 months of the effective date of Order No. 850.[6]

The Commission also determined that NERC's proposal did not address Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA),[7] with the exception of the modifications in Reliability Standard CIP-005-6, which apply to PCAs, and expressed concerns that the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.[8] The Commission accepted NERC's commitment to evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC Board of Trustees (BOT) in its resolutions of August 10, 2017. The Commission further directed NERC to file the BOT-directed final report with the Commission upon its completion.[9]

NERC filed a petition with the Commission on December 14, 2020 (Docket Number RD21-2).[10] The docket was noticed on January 7, 2021 with a 21-day comment/intervention period, ending on January 28, 2021. In response to the notice of filings, FERC received no comments. The proposed Reliability Standards improve the reliability of the Bulk Electric System ("BES") and address the Commission's directive from Order No. 850 to develop modifications to include Electronic Access Control or Monitoring Systems ("EACMS") associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability

4 Order No. 850 at P 28. These four objectives were the subject of directives from Order No. 829.
5 *Id.* P 4. EACMS are defined as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." North American Electric Reliability Corporation, Glossary of Terms Used in NERC Reliability Standards (Jan. 4, 2021) (NERC Glossary).
6 Order No. 850, 165 FERC 61,020 at P 5.
7 The NERC Glossary defines PACS as "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." NERC defines PCAs as "[o]ne or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. …"
8 Order No. 850, 165 FERC 61,020 at P 6.
9 *Id*.
10 The NERC Petition is available on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

Standards.[11] The NERC petition requests approval of proposed Reliability Standards CIP-013-2 (Cyber Security – Supply Chain Risk Management), CIP-005-7 (Cyber Security – Electronic Security Perimeter(s)), and CIP-010-4 (Cyber Security – Configuration Change Management and Vulnerability Assessments). NERC also requested approval of: (1) the associated implementation plan, violation risk factors and violation severity levels; and (2) the retirement of currently effective Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3.

Pursuant to Reliability Standard CIP-013-2 Requirement R1, responsible entities should update their supply chain risk management plans to include Electronic Access Control or Monitoring Systems and Physical Access Control Systems. The act of implementing the modified plans and procedures may result in additional documentation, as required by Reliability Standard CIP-013-2, Requirement R2. In addition to the above one-time paperwork requirements, pursuant to Reliability Standard CIP-013-1, Requirement R3, responsible entities are required to review their supply chain risk management plan and associated procedures every 15 months.

The technical requirements in Reliability Standard CIP-005-7, Requirement R3.1 and Requirement R3.2 are likely to result in documentation burden in year one to implement new reporting requirements. Reliability Standard CIP-010-4, Requirement R1.6 will require modification of certain procedures, as well as initial implementation and documentation of said procedures. The compliance-related recordkeeping requirements of the above-mentioned standards will continue on an ongoing basis beginning in year one.

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

The information collection requirements in the CIP standards apply to entities registered as the following functions: balancing authorities, distribution providers, generator operators, generator owners, interchange coordinators (or interchange authorities), reliability coordinators, transmission operators, and transmission owners. There are 1,494 unique registered entities in the NERC compliance registry as of February 5, 2021. Of this total, the Commission estimates that 343 entities (Balancing Authority [BA], Distribution Provider [DP], Generator Owner [GO], Generator Operator [GOP], Reliability Coordinator [RC], Transmission Owner [TO], and Transmission Operator [TOP]) will face an increased paperwork burden due to Docket No. RD21-2 Each of these entities is considered a "respondent" 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

11 Supply Chain Risk Management Reliability Standards, Order No. 850, 165 FERC 61,020 (2018) [hereinafter Order No. 850].

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) that relies upon any such documentation 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.

Reliability Standard CIP-013-2. Per NERC's petition, CIP-013-2 – Cyber Security - Supply Chain Risk Management[12] has the following reporting requirements:

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
- One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:
    - 1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
    - 1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
        - 1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
        - 1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
        - 1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and
        - 1.2.6. Coordination of controls for vendor-initiated remote access.

12 The applicability portion of Reliability Standard CIP-013-2 (Cyber Security - Supply Chain Risk Management) remains unchanged from CIP-013-1 and was not intentionally excluded in this supporting statement. Full details of the applicability portion can be found in the NERC petition which is available on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

Reliability Standard CIP-005-7. Per NERC's petition, CIP-005-7– Cyber Security – Electronic Security Perimeter(s) has the following reporting requirements:

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7:

- 1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
- All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
- Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
    - Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets.

- Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-005-7Table R1 – Electronic Security Perimeter and additional evidence to demonstrate implementation as described in the Measures column of the table.[13]

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible.
M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP005-7 (Remote Access Management).

- 2.1 For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
- 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.
- 2.4 Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
- 2.5 Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-7.
M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-7 (Vendor Remote Access Management for EACMS and PACS).

- 3.1 Have one or more method(s) to determine authenticated vendorinitiated remote connections.

3.2 Have one or more method(s) to terminate authenticated vendorinitiated remote connections and control the ability to reconnect.

The following applicable systems have been added to CIP-005-7 which specifies the scope of the requirements.

13 The full table can be found in Exhibit A-2 (pg. 6) of the NERC petition on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

- Part 3.1: EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity
  - Requirements: Have one or more method(s) to determine authenticated vendorinitiated remote connections.
  - Measurements: Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
- Part 3.2: EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity
  - Requirements: Have one or more method(s) to terminate authenticated vendorinitiated remote connections and control the ability to reconnect.
  - Measurements: Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems.
    - Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

Reliability Standard CIP-010-4. Per NERC's petition, CIP-010-4–Cyber Security—Configuration Change Management and Vulnerability Assessments has the following reporting requirements:

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 (Configuration Change Management).
M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-4 (Configuration Change Management).

- 1.1 Develop a baseline configuration, individually or by group, which shall include the following items:

- 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
- 1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
- 1.1.3. Any custom software installed;
- 1.1.4. Any logical network accessible ports; and
- 1.1.5. Any security patches applied.

- 1.2 Authorize and document changes that deviate from the existing baseline configuration.
- 1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change
- 1.4 For a change that deviates from the existing baseline configuration:
  - 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
  - 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
  - 1.4.3. Document the results of the verification.
  - 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration:
    - 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
    - 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
  - 1.6 Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
    - 1.6.1. Verify the identity of the software source; and
    - 1.6.2. Verify the integrity of the software obtained from the software source.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 (Configuration Monitoring).
M2 Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-4 (Configuration Monitoring)

- 2.1 Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 (Vulnerability Assessments). Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-3 (Vulnerability Assessments)

- 3.1 At least once every 15 calendar months, conduct a paper or active vulnerability assessment.
- 3.2 Where technically feasible, at least once every 36 calendar months:
    - 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and
    - 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
- 3.3 Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.
- 3.4 Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-010-3 Table R3 – Vulnerability Assessments and additional evidence to demonstrate implementation as described in the Measures column of the table.[14]

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional

14 The full table can be found in Exhibit A-3 (pg. 12) of the NERC petition through on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media.[15]
M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

The following applicable systems have been added to CIP-010-4 which specifies the scope of the requirements.

- Applicable Systems: High Impact BES Cyber Systems and their associated: 1. EACMS; and 1.2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 1.2.

PACS Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

- Requirements: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source
- Measurements: An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

Evidence Retention. Per NERC's petition, CIP-013-2 (Cyber Security–Supply Chain Risk Management), CIP-005-7 (Cyber Security–Electronic Security Perimeter(s)), CIP-010-4 (Cyber Security–Configuration Monitoring), all have the following evidence retention requirements:

- The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

15 A list of Transient Cyber Assets and Removable Media can be found in Attachment 1 of the NERC Petition which is available on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

If the information collection and record retention 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 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 adversely 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. This collection does not require industry to file the information with the Commission. We think that nearly all of the respondents are likely to make and keep related records in an electronic format. Each of the eight Regional Entities has a well-established compliance portal for registered entities to electronically submit compliance information and reports. The compliance portals allow documents developed by the registered entities to be attached and uploaded to the Regional Entity's portal. Compliance data can also be submitted by filling out data forms on the portals. These portals are accessible through an internet browser password-protected user interface.

In general, the Commission supports the use of information technology to reduce burden.

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

Filing requirements are periodically reviewed as OMB review dates arise or as the Commission may deem necessary in carrying out its regulatory responsibilities under the FPA in order to eliminate duplication and ensure that filing burden is minimized. The information collection requirements are unique to thes reliability standards 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 Reliability Standards generally do apply to small entities, depending first on their registered function(s) and then on the types of facilities they own. Nearly all the small entities[16], which are subject to the CIP 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.

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." Due to the inherent connectivity between entities that must occur to operate the Bulk-Power System, the CIP 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.

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 establishing and maintaining cyber security. The power grid would be at greater risk to cyber threats if the collection was conducted less frequently. Through periodic compliance enforcement by FERC and the ERO, responsible entities are able to identify instances of non-compliance and mitigate the identified cybersecurity risk(s), thereby improving the reliability of the bulk electric system.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

There is one special circumstance 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 often does not remove the information from the site of the entity and, in any case, returns the confidential information to the entity following the audit. This special circumstance is necessary to maintain an effective cyber-security program.

16 While it is possible for a small entity to have medium or high impact BES cyber system, it would be unlikely and have a negliable affect on the Paperwork Reduction Act (PRA) requirements.

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

FERC issued a public notice requesting comments on the NERC petition on January 7, 2021 and no comments were received.

FERC issued a Commission Letter Order (CLO) on March 18, 2021.[17]

In accordance with OMB requirements[18], the Commission published a 60-day notice (86 FR 11760) and a 30-day (86 FR 23718) notice in the *Federal Register* to the public regarding this information collection on 2/22/2021 and 5/4/2021 respectively. The Commission noted that it would be requesting a three-year extension of the public reporting burden concerning the collection of data.

The Commission received no comments on the 60-day Paperwork Reduction Act notice.

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

The Commission makes no payments or gifts to respondents as part of this collection.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

According to the NERC Rules of Procedure[19], "…a Receiving Entity shall keep in confidence and not copy, disclose, or distribute any Confidential Information or any part thereof without the permission of the Submitting Entity, except as otherwise legally required." This serves to protect confidential information submitted to NERC or Regional Entities. Responding entities do not submit the information collected due to the Reliability Standards to FERC. Rather, they submit the information to NERC or Regional Entities, or they maintain it internally. Since there are no submissions made to FERC, FERC provides no specific provisions in order to protect confidentiality.

11. PROVIDE ADDITIONAL JUSTIFICATION FOR ANY QUESTIONS OF A SENSITIVE NATURE, SUCH AS SEXUAL BEHAVIOR AND ATTITUDES, RELIGIOUS BELIEFS, AND OTHER MATTERS THAT ARE COMMONLY CONSIDERED PRIVATE.

This collection does not include any questions of a sensitive nature.

---

17 The Commission Letter Order is available on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.
18 5 CFR 1320.8(d)
19 Section 1502, Paragraph 2, available at NERC's website.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

For the hourly cost (for wages and benefits) for the reporting requirements, FERC estimates that

- 2% of the time is spent by Electrical Engineers (code 17-2071, at $70.19/hr.),
- 15% of the time is spent by Legal (code 23-0000, at $142.65/hr.),
- 31.5% of the time is spent by Information Security Analysts (Occupation Code 15-1122, at $71.47/hr.),
- 10% of the time is spent by Computer and Information Systems Managers (Occupation Code: 11-3021, at $101.58/hr.),
- 10% of the time is spent by Management (Occupation Code: 11-0000, at $97.15/hr.), and
- 31.5% of the time is spent by Management Analyst (Code: 43-0000 at $66.23/hr.).

Therefore, for reporting requirements, we use the weighted hourly cost (for wages and benefits) of $86.05.

For recordkeeping requirements, for hourly cost (for wages and benefits), we are using $41.03 for Information and Record Clerks (code 43-4199).

The estimated additional burden[20] and cost[21] for FERC-725B2 due to proposed changes (in Docket No. RD21-2) to Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 follow:

FERC-725B2, Estimated Additional Annual Burden Due to Docket No. RD21-2[1]						
Type and No. of Respondents[22]	**Type of Reporting or Recordkeeping Requirement**	**Annual No. of Respondents (A)**	**Annual No. of Responses Per Respondent (B)**	**Total No. of Annual Responses (A)x(B)=(C)**	**Average Annual Burden Hours & Cost ($) per Response (D)**	**Estimated Total Annual Burden Hrs. & Cost ($) (C)x(D)**
Reliability Standard CIP-013-2						
343 (BA, DP, GO, GOP, RC, TO, and TOP)	Reporting, Implementation (one-time in Year 1)	343	1	343	136 hrs.; $11,702.80	46,648 hrs.; $4,014,060.40
343 (BA,	Reporting	343	1	343	30 hrs.;	10,290 hrs.;

20 Burden is defined as the total time, effort, or financial resources expended by persons to generate, maintain, retain, or disclose or provide information to or for a Federal agency. For further explanation of what is included in the information collection burden, refer to 5 CFR 1320.3.

21 Costs (for wages and benefits) are based on wage figures from the Bureau of Labor Statistics (BLS) for May 2019 (at https://www.bls.gov/oes/current/naics2_22.htm) and benefits information issued March 19, 2020 (at https://www.bls.gov/news.release/ecec.nr0.htm).

22 There are 1,494 unique registered entities in the NERC compliance registry as of February 5, 2021. Of this total, we estimate that 343 entities (Balancing Authority [BA], Distribution Provider [DP], Generator Owner [GO], Generator Operator [GOP], Reliability Coordinator [RC], Transmission Owner [TO], and Transmission Operator [TOP]) will face an increased paperwork burden due to Docket No. RD21-2.

DP, GO, GOP, RC, TO, and TOP)	(ongoing starting in Year 2)				$2,581.50	$885,454.50
343 (BA, DP, GO, GOP, RC, TO, and TOP)	Recordkeeping (ongoing starting in Year 1)	343	1	343	5 hrs.; $205.15	1,715 hrs.; $70,366.45
Sub-Total for CIP-013-2[23]						**58,653 hrs.; $4,969,881.35**
Reliability Standard CIP-005-7						
343 (BA, DP, GO, GOP, RC, TO, and TOP)	Reporting, Implementation (one-time in Year 1)	343	1	343	12 hrs.; $1,032.60	4,116 hrs.; $354,181.80
343 (BA, DP, GO, GOP, RC, TO, and TOP)	Recordkeeping (ongoing starting in Year 1)	343	1	343	3 hrs.; $123.09	1,029 hrs.; $42,219.87
Sub-Total for CIP-005-7 For Year 1[24]						**5,145 hrs.; $396,401.67**
Reliability Standard CIP-010-4						
343 (BA, DP, GO, GOP, RC, TO, and TOP)	Reporting, Implementation (one-time in Yr. 1)	343	1	343	12 hrs.; $1,032.60	4,116 hrs.; $354,181.80
343 (BA,	Recordkeeping	343	1	343	3 hrs.,	1,029 hrs.;

23 The burden is 48,363 hours (which includes ongoing and one time burdens in year 1). The burden in years 2 and 3 is 12,005 hours each. Therefore, the total average annual burden for Reliability Standard CIP-013-2 over years 1-3 is 72,373 ÷ 3 = 24,124.33 hours.

24 The burden is 5,145 hours (which includes ongoing and one time burdens in year 1). The burden in years 2 and 3 is 1,029 hours each. Therefore, the total average annual burden for Reliability Standard CIP-005-7 **and** CIP-010-4 over years 1-3 is 7,203 ÷ 3 = 2,401 hours.

DP, GO, GOP, RC, TO, and TOP)	(ongoing starting in Year 1)				$123.09	$42,219.87
Sub-Total for CIP-010-4 For Year 1[24]				343		**5,145 hrs.; $396,401.67**
Sub-Total for Year 1 Burden (Includes reporting and recordkeeping)						**58,653 hrs.**
Sub-Total for Year 2 Burden (Includes reporting and recordkeeping)						**14,063 hrs.**
Sub-Total for Year 3 Burden						**14,063 hrs.**
Total Average Annual Burden Hrs. for Years 1-3, and Cost[25], due to				343		**28,926.33 hrs.; $2,555,371.72**

25 The total average cost due to RD21-2 over three years is determined by adding the costs from each Reliability Standard and dividing by 3 as follows. We multiply the costs if it is ongoing in years 1, 2 and/or 3:

- CIP-013-2: $4,014,060.40+($885,454.50*2)+ ($70,366.45*3)=$5,996,068.75 ÷ 3 = 1,998,689.58 (cont…)
- CIP-005-7: $354,181.80+ ($42,219.87*3)=$835,023.21 ÷ 3 = 278,341.07
- CIP-010-4: $354,181.80+ ($42,219.87*3)=$835,023.21 ÷ 3 = 278,341.07

Therefore, the total average annual cost is $2,555,371.72

RD21-2						

The subtotal for reporting and recordkeeping burden hours for all three standars for each year is as follows:
Year 1: 58,653 hours
Year 2: 14,063 hours
Year 3: 14,063 hours

For administrative purposes, we are averaging the one-time burden in Year 1 and ongoing burden over a three year period for each Reliability Standard. Exact calculations can be found in footnotes 23 and 24.

The total average annual burden for Reliability Standard CIP-013-2 over years 1-3 is 72,373 ÷ 3 = 24,124.33 hours. The total average annual burden for Reliability Standard CIP-005-7 and CIP-010-4 over years 1-3 is 7,203 ÷ 3 = 2,401 hours. Therefore, the total average annual burden hours for years 1-3 for all three CIP standards is (24,124.33+2,401+2,401=28,926.33) rounded to 28,926 hours.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

There are no non-labor start-up costs. All costs are discussed in question 12 and 15.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT
The Regional Entities and NERC do most of the data processing, monitoring, auditing, and compliance work for Reliability Standards. Any involvement by the Commission is covered under the FERC-725B2 (OMB Control No. 1902-0304) and is not part of this request or package. The data for FERC-725B2 is not submitted to FERC.

The Commission does incur the costs associated with obtaining OMB clearance for FERC-725B2 collection under the Paperwork Reduction Act (PRA). The PRA Administrative Cost is a Federal Cost associated with preparing, issuing, and submitting materials necessary to comply with the PRA for rulemakings, orders, or any other vehicle used to create, modify, extend, or discontinue an information collection. This average annual cost includes requests for extensions, all associated rulemakings and orders, other changes to the collection, and associated publications in the Federal Register. FERC estimates the annual cost for this effort to be $6,475. The estimated annualized cost to the Federal Government related to the data collection is shown below:

FERC-725B2	**Number of Employees (FTEs)**	**Estimated Annual Federal Cost**

Analysis of Filings	0	$0
Processing of Filings	0	$0
Paperwork Reduction Act Administrative Cost		$6,475
TOTAL		$6,475

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

As stated in Commission Letter Order,

> "NERC explains that the revised Reliability Standard will now help reduce the risk of an attacker exploiting a legitimate vendor patch management process for EACMS and PACS by requiring responsible entities to apply these protections to EACMS and PACS…
>
> [FERC] determine[s] that the proposed Reliability Standards satisfy the directive in Order No. 850 to modify these Reliability Standards to include EACMS as applicable systems. The proposed Reliability Standards also address the Commission's concern that the exclusion of PACS may leave a gap in the supply chain risk management Reliability Standards."[26]

FERC-725B2	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	1,029[27]	0	0	1,029
Annual Time Burden (Hrs.)	28,296	0	0	28,296
Annual Cost Burden ($)	0	0	0	0

The format, label, and definitions of the table above follow the Office of Management and Budget's online submittal system for information collection requests.

16. TIME SCHEDULE FOR PUBLICATION OF DATA

There is no publication of data associated with this collection of information.

17. DISPLAY OF EXPIRATION DATE

The expiration date is displayed at https://www.reginfo.gov/public/do/PRAMain

26 The Commission Letter Order is available on FERC's eLibrary system (https://elibrary.ferc.gov/eLibrary/search) by searching in Docket Number RD21-2.

27 The number of respondents is 343 per CIP standard. In this request we are discussing 3 CIP Standards. Therefore, 343*3=1,029 responses.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

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