Supporting Statement for
FERC-725B(5), Mandatory Reliability Standards: Reliability Standard CIP-003-9
(Three-year approval)

The Federal Energy Regulatory Commission (FERC or Commission) requests that the Office of Management and Budget (OMB) review and approve RD23-3-000 the information collection requirements in FERC-725B(5) under OMB Control No. 1902-NEW. This supporting statement covers the requirements of the FERC-725B(5) information collection. The reporting requirements in the FERC-725B(5) are also contained in FERC's regulations in 18 Code of Federal Regulations (CFR) Part 40. FERC is also updating information associated with other NERC Reliability Standards that fall under FERC-725B(5).

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 to the Federal Power Act (FPA)[1], 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]

Reliability Standard CIP-003-8 (up for Retirement)
Cyber Security -Security Management Controls

Reliability Standard CIP-003-9 (active)
A new cybersecurity standard that will expand supply chain risk management practices for low-impact bulk electric system cyber systems.

NERC Petition December 6, 2022
The new standard, proposed by the North American Electric Reliability Corporation (NERC) in December 2022, requires entities with bulk electric system facilities whose assets are designated low impact to have methods for determining and disabling vendor remote access. Generally, low-impact assets are generation or transmission facilities that pose a lower risk to the bulk electric system if they are compromised.
This standard improves the reliability of the grid by expanding existing security controls to provide greater visibility into electronic communication between low-impact bulk electric system

1 16 U.S.C. 824o.
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).

cyber systems and vendors. These security controls will allow detection and the ability to disable vendor remote access in the event of a known or suspected malicious communication.

Reliability Standard CIP-003-9 requires entities to adopt and maintain cyber security policies for the areas covered under the other CIP cyber security standards. The purpose of these policies is to communicate management goals, objectives, and expectations for protecting BES Cyber Systems. Proposed Reliability Standard CIP-003-9 also contains all of the requirements applicable to low impact BES Cyber Systems. Requirement R2 of CIP003-9 requires Responsible Entities to implement cyber security plans for low impact BES Cyber Systems that address the following areas: (1) cyber security awareness; (2) physical security; (3) electronic access; (4) Cyber Security Incident response; (5) Transient Cyber Asset and Removable Media malicious code risk mitigation; and (6) vendor electronic remote access security controls. The revisions in Reliability Standard CIP-003-9 improve upon Commission approved CIP-003-8 by adding new requirements focused on supply chain risk management for low impact BES Cyber Systems. Requirement R1, Part 1.2.6 requires Responsible Entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies. Requirement R2, Attachment 1, Section 6 requires Responsible Entities with assets containing low impact BES Cyber Systems that have established vendor electronic remote access to have methods for determining and disabling that vendor electronic remote access as well as one or more methods for detecting malicious communications for only that vendor electronic remote access. The requirements enhance reliability by requiring controls that grant Responsible Entities additional visibility into threats posed by supply chain risks to low impact BES Cyber Systems. The requirements also address the risks identified in NERC assessments (Exhibit E) by requiring controls around vendor electronic remote access, a potential vector of attack into BES Cyber Systems.

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

On August 8, 2005, Congress enacted the Energy Policy Act of 2005.[3] The Energy Policy Act of 2005 added a new section 215 to the Federal Power Act (FPA),[4] which requires a Commission-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards,[5] including requirements for cybersecurity protection, which are subject to

3 Energy Policy Act of 2005, Pub. L. No. 109-58, sec. 1261 *et seq.*, 119 Stat. 594 (2005).
4 16 U.S.C. 824o.
5 Section 215 of the FPA defines Reliability Standard as a requirement, approved by the Commission, to provide for reliable operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the Bulk-Power System. However, the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity. *Id.* at 824o(a)

Commission review and approval. Once approved, the Reliability Standards may be enforced by the Electric Reliability Organization subject to Commission oversight, or the Commission can independently enforce Reliability Standards.

On February 3, 2006, the Commission issued Order No. 672,[6] implementing FPA section 215. The Commission subsequently certified the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization. The Reliability Standards developed by NERC become mandatory and enforceable after Commission approval and apply to users, owners, and operators of the Bulk-Power System, as set forth in each Reliability Standard.[7] The CIP Reliability Standards require entities to comply with specific requirements to safeguard bulk electric system (BES) Cyber Systems[8] and their associated BES Cyber Assets. These standards are results-based and do not specify a technology or method to achieve compliance, instead leaving it up to the entity to decide how best to comply.

---

(3).

6 *Rules Concerning Certification of the Elec. Reliability Org.; and Procedures for the Establishment, Approval, and Enf't of Elec. Reliability Standards*, Order No. 672, 71 FR 8661 (Feb. 17, 2006), 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 71 FR 19814 (Apr. 28, 2006), 114 FERC ¶ 61,328 (2006).

7 NERC uses the term "registered entity" to identify users, owners, and operators of the Bulk-Power System responsible for performing specified reliability functions with respect to NERC Reliability Standards. *See, e.g.*, *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 FR 24594 (Apr. 25, 2012), 139 FERC ¶ 61,058, at P 46, *order denying clarification and reh'g*, 140 FERC ¶ 61,109 (2012). Within the NERC Reliability Standards are various subsets of entities responsible for performing various specified reliability functions. We collectively refer to these as "entities."

8 NERC defines BES Cyber System as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC, Glossary of Terms Used in NERC Reliability Standards, at 5 (2020), https://www.nerc.com/files/glossary_of_terms.pdf (NERC Glossary of Terms). NERC defines BES Cyber Asset as

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Id. at 4.

The Commission has approved multiple versions of the CIP Reliability Standards submitted by NERC, partly to address the evolving nature of cyber-related threats to the Bulk-Power System. High impact systems include large control centers. Medium impact systems include smaller control centers, ultra-high voltage transmission, and large substations and generating facilities. The remainder of the BES Cyber Systems are categorized as low impact systems. Most requirements in the CIP Reliability Standards apply to high and medium impact systems; however, a technical controls requirement in Reliability standard CIP-003, described below, applies only to low impact systems.

The Commission is currently revising CIP-003 on this submission of Docket No. RD23-3-000 to update CIP-003-8 to CIP-003-9.

Reliability Standard CIP-003-9 Security Management Controls: requires entities to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to mis-operation or instability on the Bulk-Power System. Specifically, the Reliability Standard CIP-003-9 is revised to add requirements for entities to adopt mandatory security controls for vendor electronic remote access used at low impact BES Cyber Systems. It is part of the implementation of the Congressional mandate of the Energy Policy Act of 2005 to develop mandatory and enforceable Reliability Standards to better ensure the reliability of the nation's Bulk-Power System.

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

This collection does not require industry to file the information with the Commission. However, FERC-725B(5) does contain information collection and record retention requirements for which using current technology is an option.

The information technology to meet the information collection requirements is not specifically covered in the Reliability Standard.

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 Commission periodically reviews filing requirements concurrent with OMB review or as the Commission deems necessary to eliminate duplicative filing and to minimize the filing burden.

The Commission is unaware of any other source of information related to bulk-electric system physical security.

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

In general, small entities may reduce their burden by taking part in a joint registration organization or a coordinated functional registration. These options allow a small entity to share the compliance burden with other entities and, thus, to minimize their own compliance burden. Detailed information regarding these options is available in NERC's Rule of Procedure at Sections 507 and 508.[9]

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

The paperwork requirements are related with documenting compliance with substantive requirements (including the preparation of a physical security plan) and maintaining such documents. The frequency of the paperwork requirements was vetted and approved by industry consensus in the NERC standard development process and is ultimately meant to support the reliability of the bulk electric system.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

There are no special circumstances related to the FERC-725B(5) information collection.

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 comments.[10] The NERC-approved Reliability Standards were then submitted by NERC to the FERC for review and approval.

In accordance with OMB requirements, the Commission published a 60-day notice[11] and a 30-day notice[12] to the public regarding this information collection on 3/30/2023 and 6/8/2023

9 http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20161031.pdf
10 Details of the ERO standards development process are available on the NERC website at http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.
11 88 FR 19124
12 88 FR 37525

respectively. The Commission received no comments from the public in response to either published notice regarding the FERC-725B(5) information collection.

Notice of Filing and Responsive Pleadings

As required by Section 39.5(a) of the Commission's regulations, this petition presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history and complete record of development (Exhibit G), and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 6725 (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on November 16, 2022.

I. SUMMARY

Entities' increasing reliance on microprocessor-driven devices to operate the BES introduces cyber security supply chain risks. These devices help entities to have better responsive control over BES equipment but also, if compromised through supply chain vulnerabilities, could impact BES reliability. As such, NERC's cyber security Critical Infrastructure Protection ("CIP") Reliability Standards seek to mitigate cyber security risks, including supply chain risks, to BES Facilities, systems, and equipment. To address these risks, the cyber security CIP standards focus on protections around BES Cyber Systems located at or associated with BES Facilities, systems, and equipment. Responsible Entities categorize BES Cyber Systems as low, medium, or high impact based on the characteristics of their BES Facilities, systems, and equipment. Depending on the assigned impact level, Responsible Entities then apply corresponding requirements from the CIP Reliability Standards to their BES Cyber Systems or the assets containing those BES Cyber Systems. Since the development of the original Supply Chain Standards, NERC has continued to focus on supply chain risk management as it relates to the reliability of the Bulk Power System ("BPS"). In addition to Reliability Standards requirements, NERC has leveraged several tools to address these risks, including NERC Alerts, a joint white paper with FERC staff, and an initiative dedicated to supply chain risk mitigation, among other activities. As part of this continued focus on supply chain issues, NERC conducted a study to evaluate supply chain risks associated with assets containing low impact BES Cyber Systems and collected data to assess whether further revisions to the CIP Reliability Standards were needed to address these risks. Based on the data collected, NERC determined that low impact BES Cyber Systems, while still low impact to the BES, could present a greater risk if numerous assets were compromised through remote access. To that end, NERC recommended revisions to the CIP Reliability Standards to address supply chain risk management for assets containing low impact BES Cyber Systems.

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

There are no gifts or payments given to the respondents.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

According to the NERC Rules of Procedure,[13] "…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 under the Reliability Standard to FERC. Rather, 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.

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

The Commission bases its paperwork burden estimates on the changes in paperwork burden presented by the proposed revision to CIP Reliability Standard CIP-003-9 as compared to the current Commission-approved Reliability Standard CIP-003-8. As discussed above, the immediate order addresses the area of modification to the CIP Reliability Standards: adopting mandatory security controls for vendor electronic remote access used at low impact BES Cyber Systems.

The CIP Reliability Standards within FERC-725B (Currently in 725B(5) for a temporary placeholder while 725B is pending at OMB), viewed as a whole, implement a defense-in-depth approach to protecting the security of BES Cyber Systems at all impact levels.[14] The CIP Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems.[15] The NERC Compliance Registry, as of January 4, 2023, identifies approximately 1,592 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,579 entities will face an increased paperwork burden under Reliability Standard CIP 003-9, estimating that a majority of these entities will have one or more low impact BES Cyber Systems. Based on these assumptions, the Commission estimates the total annual burden and cost as follows:

13 Section 1502, Paragraph 2, available at NERCs website.

14 Order No. 822, 154 FERC ¶ 61,037 at 32.

15 *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC ¶ 61,040, at P 72 (2008); *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).

RD23-3-000 Commission Order **(Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards CIP-003-9)**						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response[16] (4)**	**Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)**	**Cost per Respondent ($) (5)÷(1)**
Create vendor remote access policy (one-time)[17]	1,579	1	1,579	60 hrs. $5,340	94,740 hrs. $8,431,860	$5,340
Updates and reviews of vendor remote access policy (ongoing)	1,579	1	1,579	3.5 hrs. $311.50	5,527 hrs. (rounded) $491,903	$311.50

16 The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for 2022 found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm):

Legal (Occupation Code: 23-0000): $145.35
Electrical Engineer (Occupation Code: 17-2071): $77.02
Office and Administrative Support (Occupation Code: 43-0000): $43.62

($145.35 + $77.02 + $43.62) ÷ 3 = $88.66. The figure is rounded to $89.00 for use in calculating wage figures in this Commission Order.

17 This one-time burden applies in Year One only.

Total burden for FERC-725B(5) under CIP-003-9			3,158		100,267 hrs. $8,923,763	

The one-time burden of 94,740 hours that only applies for Year 1 will be averaged over three years (94,740 hours ÷ 3 = 31,580 hours/year over three years). The number of responses is also averaged over three years (1,579 responses ÷ 3 = 526.33 responses/year).

The responses and burden hours for Years 1-3 will total respectively as follows for Year 1 one-time burden:

Year 1: 526.33 responses; 31,580 hours

Year 2: 526.33 responses; 31,580 hours

Year 3: 526.33 responses; 31,580 hours

The responses and burden hours for Years 1-3 will total respectively as follows for Ongoing and beyond: 1,579 responses and 5,527 hours

The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: $8,431,860 (Onetime)
- Years 2 and 3: $491,903 (Ongoing)

The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices (e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to policy development, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

There are no start-up or other non-labor costs.

Total Capital and Start-up cost: $0
Total Operation, Maintenance, and Purchase of Services: $0

All of the costs related to the FERC-725B(5) information collection are associated with burden hours (labor) and described in Questions #12 and #15 in this supporting statement.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The Regional Entities and NERC do most of the data processing, monitoring, and compliance work for Reliability Standards. Any involvement by the Commission is covered under the FERC-725 collection (OMB Control No. 1902-0225) and is not part of this request or package.

The estimated annualized cost to the Federal Government for FERC-725B(5) follows:

FERC-725B(5)- CIP standards	Number of Employees (FTEs)	Estimated Annual Federal Cost
FERC-725B(5) Analysis and Processing of filings	0	$0
Paperwork Reduction Act Administrative Cost[18]		$7,694
TOTAL		$7,694

Based on the above table, the total federal cost for FERC-725B(5) is $7,694.

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

FERC-725B(5) is a new collection created as a temporary placeholder. Since FERC-725B is currently held up at OMB due to a current rulemaking under RM22-19. The currently approved burden for FERC-725B is currently 241,001 annual burden responses and 2,162,901 annual burden hours. Once the OMB number for FERC-725B is available the current burden below will then be added back into FERC-725B(5).The one-time burden of 94,740 hours that only applies for Year 1 will be averaged over three years (94,740 hours ÷ 3 = 31,580 hours/year over three

18 The PRA Administrative Cost is a Federal Cost associated with preparing, issuing, and submitting materials necessary to comply with the Paperwork Reduction Act (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 other changes to the collection.

years). The number of responses is also averaged over three years (1,579 responses ÷ 3 = 526.33 responses/year).
The responses and burden hours for Years 1-3 will total respectively as follows for Year 1 one-time burden:
Year 1: 526.33 responses; 31,580 hours
Year 2: 526.33 responses; 31,580 hours
Year 3: 526.33 responses; 31,580 hours
The responses and burden hours for Years 1-3 will total respectively as follows for Ongoing and beyond: 1,579 responses and 5,527 hours

FERC-725b(5)	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	2,105	0	0	2,105
Annual Time Burden (Hr.)	37,107	0	0	37,107
Annual Cost Burden ($)	$0	$0	$0	$0

16. TIME SCHEDULE FOR PUBLICATION OF DATA

There is no tabulating, statistical or tabulating analysis or publication plans for the collection of information.

17. DISPLAY OF EXPIRATION DATE

The expiration dates are displayed in a table posted on www.ferc.gov at https://www.ferc.gov/information-collections.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.