

Supporting Statement for
FERC-725U, Mandatory Reliability Standards: Reliability Standard CIP-014
(Three-year approval and RD22-3 for extension requested)

The Federal Energy Regulatory Commission (FERC or Commission) requests that the Office of Management and Budget (OMB) review and approve RD-22-3-000 the information collection requirements in FERC-725U under OMB Control No. 1902-0274. This supporting statement covers the requirements of the FERC-725U information collection. The reporting requirements in the FERC-725U 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-725U.

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. EPAAct 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-014-1 (inactive as of 10/1/2015)

On 11/20/2014, FERC issued an order³ approving Reliability Standard CIP-014-1. Reliability Standard CIP-014-1 enhanced physical security measures for the critical Bulk-Power System facilities and lessened the overall vulnerability of the Bulk-Power System against physical attacks.

Reliability Standard CIP-014-2 (inactive as of 6/16/2022)

On 7/14/2015, FERC issued a letter order approving Reliability Standard CIP-014-2 (the current version of the Reliability Standard). Reliability Standard CIP-014-2 modified Reliability Standard CIP-014-1 by removing the term “widespread” from Requirement R1. Removing the term ensured that:

- Applicable entities identify appropriate critical facilities under Requirement R1, and
- The electric reliability organization enforces the CIP-014-2 Reliability Standard in a more consistent manner.

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).

3 Order No. 802 (79 FR 70069, 11/25/2014)

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

Section 215 and Mandatory Reliability Standards

Section 215 of the Federal Power Act (FPA) requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. The ERO is obligated to file each Reliability Standard or modification to a Reliability Standard that it proposes to be made effective with the Commission.⁴ Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.⁵ Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,⁶ and subsequently certified NERC.⁷

Currently Effective Reliability Standard CIP-014-2

Reliability Standard CIP-014-2, which applies to transmission owners and transmission operators, is designed to “identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.”⁸ Pursuant to the Reliability Standard, transmission owners must perform an initial and subsequent risk assessments to identify the transmission stations and substations that, if rendered inoperable or damaged could result in instability, uncontrolled separation, or cascading within an Interconnection, and is subject to a third-party verification. Transmission owners that control identified facilities must conduct an evaluation of the potential threats and vulnerabilities of a physical attack to transmission stations and substation, as well as primary control centers, develop and implement a documented physical security plan and have a third-party review of the evaluation.

NERC Petition for Modifications to the Compliance Section of Reliability Standard CIP-014

NERC proposes to remove section C.1.1.4., Additional Compliance Information, from the compliance section of the currently effective Reliability Standard CIP-014-2 (Physical Security) that requires all evidence demonstrating compliance with this Reliability Standard to be retained at the transmission owner’s or transmission operator’s facility in order to protect the entity’s

4 16 U.S.C. 824o(d)(1).

5 Id. 824o(e).

6 Rules Concerning Certification of the Elec. Reliability Org.; & Procedures for the Establishment, Approval, & Enforcement of Elec. Reliability Standards, Order No. 672, 114 FERC ¶ 61,104, order on reh’g, Order No. 672-A, 71 FR 19814 (April 18, 2006), 114 FERC ¶ 61,328 (2006).

7 N. Am. Elec. Reliability Corp., 116 FERC ¶ 61,062, order on reh’g and compliance, 117 FERC ¶ 61,126 (2006), aff’d sub nom. Alcoa, Inc. v. FERC, 564 F.3d 1342 (D.C. Cir. 2009).

8 NERC Reliability Standard CIP-014-2 (Physical Security), Purpose.

confidential information.⁹ NERC states that the proposed change applies only to the compliance section of Reliability Standard CIP-014-2, and proposes no changes in the mandatory and enforceable Requirements of Reliability Standard CIP-014-2. According to NERC, the provision presents challenges to effective and efficient compliance monitoring and is not necessary to protect the confidentiality of Reliability Standard CIP-014-2 compliance evidence.¹⁰

NERC states that the “Additional Compliance Information” provision in the compliance section of CIP-014 was added to address heightened concerns regarding the protection of CIP-014 evidence. However, NERC has determined that it should no longer treat CIP-014 evidence any differently than other sensitive evidence it collects during its Compliance Monitoring and Enforcement Program (CMEP) activities.¹¹ With the advent of the ERO Secure Evidence Locker (SEL), NERC asserts that it has a secure means of collecting and analyzing CIP-014 evidence in the same manner as any other sensitive evidence collected as part of CMEP activities.¹⁴

NERC explains that it will no longer treat Reliability Standard CIP-014 evidence any differently than other sensitive evidence it collects during its compliance activities.¹² NERC plans to use its SEL to support data and information handling, and it explains that it has developed the SEL for temporary storage of all registered entity compliance evidence.¹³ According to NERC, the SEL enables a registered entity to securely submit evidence through an encrypted session; the evidence is encrypted immediately upon submission, securely isolated per registered entity, never extracted, never backed up, and subject to proactive and disciplined destruction policies. NERC submits that the SEL provides security advantages to ensure proper protection and chain-of-custody management of the submitted evidence for CIP-014 compliance.

Procedure and Substantive Matters

Procedural Matters

Pursuant to Rule 214 of the Commission’s Rules of Practice and Procedure, 18 CFR § 385.214 (2021), EEI’s timely, unopposed motion to intervene serve to make it a party to this proceeding.

Rule 213(a)(2) of the Commission’s Rules of Practice and Procedure, 18 CFR § 385.213(a)(2) (2021), prohibits an answer to a protest or answer unless otherwise ordered by the decisional authority. We accept NERC’s and EEI’s answers because they have provided information that assisted us in our decision-making process.

9 NERC Petition at 1. Section C.1.1.4., Additional Compliance Information states:
Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner’s and Transmission Operator’s facilities.

10 NERC Petition at 1.

11 Id. at 5-6.

12 Id.

13 Id. at 6.

Substantive Matters

As discussed below, we find that the removal of the evidence retention provision in section C.1.1.4 of the compliance section of Reliability Standard CIP-014-2 is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The modification will allow NERC to monitor compliance more effectively without compromising the confidentiality of sensitive information. Accordingly, we approve NERC's petition.

Reliability Standard CIP-014-2, compliance section C.1.1.4., Additional Compliance Information, currently requires compliance personnel and auditors (and enforcement staff if a potential noncompliance is identified) to be physically present at an entity's facility to review evidence of compliance. As NERC's petition explains, this requirement presented challenges during the pandemic, when auditors could not access certain entities' facilities in person and in some instances were prevented from reviewing the evidence remotely.¹⁴

We recognize that Reliability Standard CIP-014-2 requires data collection for industry's sensitive assets and that therefore the data should be handled in a secure manner. However, while section C.1.1.4 may have provided necessary protection in the past, we are persuaded by NERC's explanation that its SEL now offers a secure and more flexible alternative for compliance evidence collection and review for Reliability Standard CIP-014-2.

Moreover, we are not persuaded by EEI's comments seeking to retain the on-site viewing requirement. First, contrary to EEI's suggestion in its comments, the use of the SEL is not novel and untested. In NERC's petition requesting funding for the SEL, which was filed in June 2020, NERC explained that the use of an evidence locker was a practice already in place for at least two Regional Entities to collect evidence associated with Critical Infrastructure Protection (CIP) Reliability Standards.¹⁵ Before deciding to implement the SEL, NERC consulted with industry and discussed security concerns related to evidence collection.¹⁶ Also, NERC has been using the SEL to access compliance evidence for the other CIP Reliability Standards, which indicates that it is a well-established and secure method of evidence review. Restricting auditor review to on-site only when there is a secure alternative impairs the auditor's ability to perform in-depth review of the evidence and could result in increased risk due to lack of adequate or timely compliance monitoring.

Further, we are not persuaded by EEI's argument that the SEL increases the risk of aggregated industry information falling into the hands of a nation-state or bad actor. Once evidence is submitted through an SEL encrypted session, it is immediately encrypted and cannot be extracted, is not backed up, and is subject to proactive and disciplined destruction policies, as

¹⁴ NERC Petition at 7; NERC Answer at 3.

¹⁵ NERC, Request of the North American Electric Reliability Corporation to expend funds to develop the ERO Enterprise Secure Evidence Locker, Docket No. RR19-8-001, at 4 (filed June 8, 2020) (NERC 2020 Filing); N. Am. Elec. Reliability Corp., Docket No. RR19-8-001 (June 22, 2020) (delegated order).

¹⁶ NERC 2020 Filing at 5.

well as being separated by registered entity.¹⁷ NERC explained that it will remove the information from the SEL when the CMEP engagement concludes.¹⁸

Finally, as stated by NERC, entities can structure their own SELs that adhere to their security measure requirements. EEI argues that some registered entities may be unable to use their own SELs to submit compliance information if NERC or Regional Entity compliance personnel are unable or unwilling to meet the SEL security access requirements.¹⁹ However, EEI provides no specific evidence of such situations for other CIP compliance monitoring engagements or whether they have led to increased risk of evidence being compromised. We find unpersuasive EEI's objections to NERC's offering of a flexible approach to accommodate entities.

Therefore, we find that the removal of the evidence retention provision in section C.1.1.4 of the compliance section of Reliability Standard CIP-014-2 will allow NERC to monitor compliance more effectively without compromising the confidentiality of sensitive information. Accordingly, we approve NERC's petition and accept the proposed Reliability Standard CIP-014-3, to become effective on the date of issuance of this order.

CIP-014-3

In terms of information collection requirements, an applicable entity must create or maintain documentation showing compliance, when appropriate, with each requirement of the Reliability Standard. Reliability Standard CIP-014-3 has six requirements:

- Requirement R1 requires applicable transmission owners (TO) to perform risk assessments on a periodic basis²⁰ to identify their transmission stations and transmission substations that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or cascading within an Interconnection. Requirement R1 also requires transmission owners to identify the primary control center that operationally controls each of the identified transmission stations or transmission substations. Examples of acceptable evidence may include dated written or electronic documentation of the risk assessment of its transmission stations and transmission substations (existing

17 NERC Answer at 2.

18 Id. at 2-3.

19 Id.

20 The frequency is detailed in the Reliability Standard. For example, R1 states in part:

“1.1 Subsequent risk assessments shall be performed:

At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. “

and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1.

- Requirement R2 requires that each applicable transmission owner have an unaffiliated third-party with appropriate experience verify the risk assessment performed under Requirement R1. Requirement R2 states that the transmission owner must either modify its identification of facilities consistent with the verifier's recommendation or document the technical basis for not doing so. In addition, Requirement R2 requires each transmission owner to implement procedures for protecting sensitive or confidential information made available to third-party verifiers or developed under the Reliability Standard from public disclosure. Examples of acceptable evidence may include dated written or electronic documentation that the transmission owner completed an unaffiliated third-party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3.
- Requirement R3 requires the transmission owner to notify a transmission operator (TOP) that operationally controls a primary control center identified under Requirement R1 of such identification to ensure that the transmission operator has notice of the identification so that it may timely fulfill its obligations under Requirements R4 and R5 to protect the primary control center. Examples of acceptable evidence may include dated written or electronic communications that the transmission owner notified each transmission operator, as applicable, according to Requirement R3.
- Requirement R4 requires each applicable transmission owner and transmission operator to conduct an evaluation of the potential threats and vulnerabilities of a physical attack on each of its respective transmission stations, transmission substations, and primary control centers identified as critical in Requirement R1. Examples of evidence may include dated written or electronic documentation that the transmission owner or transmission operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective transmission station(s), transmission substation(s) and primary control center(s) as specified in Requirement R4.
- Requirement R5 requires each transmission owner and transmission operator to develop and implement documented physical security plans that cover each of their respective transmission stations, transmission substations, and primary control centers identified as critical in Requirement R1. Examples of evidence may include dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified transmission station(s), transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating implementation of the physical security plan.
- Requirement R6 requires that each transmission owner and transmission operator subject to Requirements R4 and R5 have an unaffiliated third-party with appropriate experience review its Requirement R4 evaluation and Requirement R5 security plan. Requirement

R6 states that the transmission owner or transmission operator must either modify its evaluation and security plan consistent with the recommendation, if any, of the reviewer or document its reasons for not doing so. In addition, Requirement R6 requires each transmission owner to implement procedures for protecting sensitive or confidential information made available to third-party reviewers or developed under the Reliability Standard from public disclosure. Examples of evidence may include written or electronic documentation that the transmission owner or transmission operator had an unaffiliated third-party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3.

Evidence Retention

Transmission owners and transmission operators must keep data or evidence to show compliance with the standard for three years unless directed by its Compliance Enforcement Authority. If a responsible entity is found non-compliant, it must keep information related to the non-compliance until mitigation is complete and approved, or for the three years, whichever is longer.

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-725U 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 508.²¹

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-725U 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.²² 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 notice²³ and a 30-day notice²⁴ to the public regarding this information collection on 6/24/2022 and 9/08/2022 respectively. The Commission received no comments from the public in response to either published notice regarding the FERC-725U information collection.

21 http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20161031.pdf

22 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.

23 87 FR 37847

24 87 FR 54991

Notice of Filing and Responsive Pleadings

Notice of NERC's February 16, 2022 Petition was published in the *Federal Register*, 87 FR 11061 (Feb.28, 2022), with interventions and protests due on or before March 15, 2022. The Edison Electric Institute (EEI) filed a timely motion to intervene and comments. On March 21, 2022, NERC submitted a request to submit reply comments and reply comments (NERC Answer). On March 30, 2022, EEI filed a motion for leave to answer and answer (EEI Answer).

EEI opposes NERC's petition and maintains that Reliability Standard CIP-014 requires data collection for industry's most sensitive assets and, therefore, the compliance provision should be retained so that NERC continues to review compliance evidence for this Reliability Standard only on-site at the registered entities for the most sensitive data.²⁵ EEI explains that the information retained under this compliance requirement is of a critical and highly sensitive nature, and some information provided for Reliability Standard CIP-014 compliance is only available to a small set of personnel on a need-to-know basis within EEI member companies.²⁶ According to EEI, its members go to great lengths to protect the identity of the assets and other sensitive information by using alternative anonymous names both in internal and external discussions. Further, EEI expresses security concerns related to the use of SEL, arguing that the SEL increases the risk of aggregated industry information falling into the hands of a nation state or bad actor.²⁷ EEI argues that ease of access cannot take precedence over the safety, security, and reliability of the electric grid.

NERC asserts in its answer that the proposed modification would not decrease the protection of any highly sensitive compliance evidence, but it is needed to ensure compliance monitoring with Reliability Standard CIP-014.²⁸ Among other arguments, NERC explains that there will be limited CIP-014 evidence aggregated in the SEL at any given time.²⁹ Further, NERC elaborates that a registered entity may choose to develop its own SEL rather than use NERC's SEL, or use NERC's exceptions process, which allows registered entities to collaborate with the compliance authority on alternative submittal methods.

Finally, NERC states that over the last two years, due to pandemic restrictions, in some instances registered entities refused on-site access for compliance monitoring.³⁰ In addition, certain entities also refused to allow a review of evidence using a secure videoconferencing platform. NERC believes that "[t]he end result was increased risk, in certain instances, because [NERC and the Regional Entities] had no mechanism with which to monitor compliance with CIP-014 until the entity, at its own discretion, lifted its pandemic-related restriction."³¹

In its answer, EEI argues that more flexibility should be given to registered entities to select the most secure methods for providing CIP-014 compliance data. In particular, EEI states that, if

25 EEI Comments at 1.

26 Id. at 5.

27 Id.

28 NERC Answer at 1.

29 Id. at 2-3.

30 Id. at 3-4.

31 Id. at 4.

agreed to by a registered entity's Compliance Enforcement Authority, "secure videoconferencing is an attractive and equally effective and efficient alternative to using the ERO SEL and one that EEI members would welcome."³² EEI notes, however, that certain entities may prefer to use their own videoconferencing tools, as opposed to an ERO-based tool, "because in doing so they have an understanding of, and confidence in, the security measures that have been implemented."³³ Further, because many registered entities' corporate security access management programs require training, background checks, and monitoring of third-party access, EEI believes that some registered entities may be unable to use their own SEL to submit compliance information if NERC or Regional Entity compliance personnel are unable or unwilling to meet their SEL security access requirements.³⁴ EEI also expresses concern with the length of time NERC will keep compliance information in the SEL, as entities have no way of verifying whether it has been deleted.

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,³⁵ "...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 number of respondents below is based on an estimate of the NERC compliance registry for

³² EEI Answer at 2.

³³ Id.

³⁴ Id. at 2-3.

³⁵ Section 1502, Paragraph 2, available at NERCs website.

transmission owners and transmission operator. The Commission based its paperwork burden estimates on the NERC compliance registry as of May 6, 2022. According to the registry, there are 326 transmission owners and 18 transmission operators not also registered as transmission owners. The estimate is based on a zero change in burden from the current standard (removal of C.1.1.4) to the standard approved in this Order. The Commission based the burden estimate on staff experience, knowledge, and expertise.

For the new Reliability Standard CIP-014-3, the burden for entities remains the same as they will still need to provide the same evidence to demonstrate compliance whether it is kept on-site or loaded electronically into the SEL. No comments were received that expressed a change in the manhour burden associated with the use of SEL.

Burden Estimates: The Commission estimates the changes in the annual public reporting burden and cost³⁶ as indicated below:

FERC-725U: (Mandatory Reliability Standards: Reliability Standard CIP-014) Change in Burden						
	Number of Respondents³⁷ (1)	Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden Hours & Cost Per Response (4)	Total Burden Hours & Total Cost (3)*(4)=(5)	Average Cost per Respondent (5)÷(1)
Change Annual Reporting and Recordkeeping	344	1	344	32.71 hrs.; \$2,845.77	11,252.24 hrs.; \$978,944.88	\$2,845.77
TOTAL FERC-725U	344	1	344	32.71 hrs.; \$2,845.77	11,254.24 hrs.; \$978,944.88	\$2,845.77

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

³⁶ FERC staff estimates that industry costs for salary plus benefits are similar to Commission costs. The FERC 2021 average salary plus benefits for one FERC full-time equivalent (FTE) is \$180,703/year (or \$87.00/hour) posted by the Bureau of Labor Statistics for the Utilities sector (available at https://www.bls.gov/oes/current/naics3_221000.htm).

³⁷ The total number (344) of transmission owners (326) plus transmission operators (18) not also registered as owners, this represents the unique US entities (taken from data as of May 6, 2022).

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-725U 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-725U follows:

FERC-725U- CIP standards	Number of Employees (FTEs)	Estimated Annual Federal Cost
FERC-725U Analysis and Processing of filings	0	\$0
Paperwork Reduction Act Administrative Cost ³⁸		\$8,279
TOTAL		\$8,279

Based on the above table, the total federal cost for FERC-725U is \$8,279.

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

Each requirement (including record-keeping requirements) in CIP-014-3 have been updated to reflect the normal fluctuations in hours and responses.³⁹ A increase of 8 in responses and increase of 263 in burden hours. There is no net change to burden due to Docket RD22-3 (removing C1.1.4).

FERC-725U	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion

³⁸ 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.

³⁹ The hourly burden for each CIP-014-3 requirement was established/approved in CIP-014-3

Annual Number of Responses	344	336	+8	0
Annual Time Burden (Hr.)	11,254	10,991	+263	0
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 ferc.gov at <http://www.ferc.gov/docs-filing/info-collections.asp>.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.