Supporting Statement for
FERC-725B3[1] (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards), as modified by the Order in Docket No. RD19-3-000

The Federal Energy Regulatory Commission (Commission or FERC) requests that the Office of Management and Budget (OMB) review and approve the FERC-725B3 information collection (Mandatory Reliability Standards for Critical Infrastructure Protection [CIP] Reliability Standards) as modified in Docket No. RD19-3-000.

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[2] 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.[3]

Pursuant to section 215(d)(2) of the FPA[4] , FERC approved Reliability Standard CIP-008-6, its associated implementation plan, violation risk factors and violation severity levels, and the revised definitions of Cyber Security Incident and Reportable Cyber Security Incident. FERC determined that the proposed Reliability Standard and revised definitions satisfy the directive in Order No. 848 to broaden mandatory reporting to include Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's electronic security perimeter or associated electronic access control

1 Commission staff is using the FERC-725B3 as a temporary "place holder" information collection number for this Supporting Statement. FERC-725B information collection (OMB Control No. 1902-0252) is pending review at OMB in an unrelated item, and only one item per OMB Control No. can be pending OMB review at a time. In order to submit this timely, to OMB, we are using a temporary place holder information collection number. The earlier version of Reliability Standard CIP-008-5 is part of FERC-725B. This Supporting Statement addresses the added burden caused by this order in RD19-3.
2 16 U.S.C. § 824o.
3 *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).
4 16 U.S.C.§ 824o(d)(2).

or monitoring systems, as well as modifications to specify the required information in Cyber Security Incident reports, their dissemination, and deadlines for filing reports.

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

The Reliability Standard CIP-008-6 broadens the mandatory reporting of Cyber Security Incidents and thus addresses the concern that currently-effective Reliability Standard CIP-008-5 may not encompass the full scope of cyber-related threats to the Bulk-Power System.[5] As a predicate to the augmented reporting requirements in Reliability Standard CIP-008-6, NERC proposed revised NERC Glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. NERC explained that, by applying the revised definitions, Cyber Security Incidents (i.e. attempts to compromise) and Reportable Cyber Security Incidents (i.e. actual compromises) will be reported under Reliability Standard CIP-008-6.

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

The use of current or improved technology and the medium are not covered in Reliability Standards and are therefore left to the discretion of each respondent. Commission staff thinks that nearly all the respondents are likely to make and keep related records in an electronic format. 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.

This collection does not require industry to file the information with the Commission

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 to eliminate duplication and ensure that filing burden is minimized. There are no

5 *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018).

similar sources for information available that can be used or modified for these reporting purposes.

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

There are 1,414 unique registered entities in the NERC compliance registry as of May 24, 2019. Of this total, we estimate that 288 entities will face an increased burden[6] due to the Order in RD19-3.

The Reliability Standard does not contain provisions for minimizing the burden of the collection for small entities. The requirements in Reliability Standard CIP-008-6 apply to 288 applicable entities. However, small entities generally can reduce their burden by taking part in a joint registration organization or a coordinated function registration. These options allow an entity to share its compliance burden with other similar entities. Detailed information regarding these options is available in NERC's Rules of Procedure at section 1502.2, available at NERCs website.

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

The consequences of not collecting the data associated with this Reliability Standard may result in an understatement of the true scope of cyber-related threats to the Bulk-Power System.

7. EXPLAIN ANY SPECIAL CIRCUMSTANCES RELATING TO THE INFORMATION COLLECTION

FERC-725B3 information collection has no special circumstances.

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

In accordance with OMB requirements[7], the Commission published a 60-day notice[8] to the public regarding this information collection on 6/26/2019. Within the public notice, the Commission noted that it would be requesting a three-year extension of the public

6 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 C.F.R. § 1320.3 (2019).

7 5 CFR 1320.8(d)
8 84 FR 30105

reporting burden with no change to the existing requirements concerning the collection of data. FERC received no comments.

FERC is also publishing a 30-day Notice in the Federal Register to provide the public with another opportunity to comment.

9. EXPLAIN ANY PAYMENT OR GIFTS TO RESPONDENTS

The Commission does not make any payments or gifts to respondents.

10. DESCRIBE ANY ASSURANCE OF CONFIDENTIALITY PROVIDED TO RESPONDENTS

According to section 1502.2 of the NERC Rules of Procedure, "…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."[9] This serves to protect confidential information submitted to NERC or Regional Entities.

Responding entities do not submit to the Commission the information collected in compliance with this Reliability Standard. Rather, they submit the information to the Electricity Information Sharing and Analysis Center and the Department of Homeland Security's National Cybersecurity and Communications Integration Center. Since there are no submissions made to FERC, FERC provides no specific provisions in order to protect confidentiality.

The only submission received by the Commission, according to NERC standards is an annual anonymized, public summary of the reports submitted to E-ISAC and ICS-CERT, or its successor. This report will include: (1) the functional impact, where possible to determine, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident. This burden is addressed in FERC-725B.

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

9 NERC's Rules of Procedure are available on its website.

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

12. ESTIMATED BURDEN OF COLLECTION OF INFORMATION

NERC Reliability Standard CIP-008-6 will result in one-time and ongoing increases to burden in the reporting requirements imposed on Balancing Authority (BA), Distribution Provider (DP), Generator Operator (GOP), Generator Owner (GO), Reliability Coordinator (RC), Transmission Operator (TOP), and Transmission Owner (TO).

The burden of the current version of the standard, which is being replaced, is approved under FERC-725B (for reporting and recording keeping requirements). The new, approved version of the standard (submitted in the FERC-725B3 information collection) will impose an additional burden (over the currently approved burden estimate). The below table shows the net increase after this Order becomes effective. The annual additional estimated burden and cost[10] for FERC-725B3 due to this approved standard follow:

FERC-725B3, in Order in Docket No. RD19-3-000[11] **(Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards)**

10 The estimated hourly cost (salary plus benefits) is based on the figures for May 2018 posted by the Bureau of Labor Statistics for the Utilities sector (available at http://www.bls.gov/oes/current/naics2_22.htm) and December 2018 for benefits information (at http://www.bls.gov/news.release/ecec.nr0.htm). The hourly estimates for salary plus benefits are:

-Legal (Occupation Code: 23-0000): $143.47
-Information Security Analysts (Occupation Code 15-1122): $61.46
-Computer and Information Systems Managers (Occupation Code: 11-3021): $96.37
-Management (Occupation Code: 11-0000): $94.15
-Electrical Engineer (Occupation Code: 17-2071): $66.80
-Management Analyst (Code: 13-1111): $63.23

These various occupational categories are weighted as follows: [($94.15(.10) + ($61.46)(.315) + ($66.80)(.02) + ($143.47)(.15) + ($96.37)(.10) + ($63.23)(.315)] = $81.19. The figure is rounded to $81.00/hour for use in calculating cost figures.

11 The burden table in this supporting statement corrects the mathematical error in the burden table that was published in the order in Docket No. RD19-3-000.

	Number of Respondents[12] (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden (Hrs.) & Cost Per Response ($) (4)	Total Annual Burden Hours & Total Annual Cost ($) (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
Update internal procedures to comply with augmented reporting requirements. (one-time)[13] (R1-R4)[14]	288	1	288	50 hrs.; $4,050	14,400 hrs.; $1,166,400	$4,050
Annual cyber security incident plan review (ongoing)[15] (R2.1)	288	1	288	10 hrs.; $810	2,880 hrs.; $233,280	$810
Update cyber security incident plan per review findings (ongoing) [13] (R3)	288	1	288	10 hrs.; $810	2880 hrs.; $233,280	$810
Incident reporting burden (ongoing) (R4)	288	12	3,456	12 hrs.; $972	41,472 hrs; $3,359,232	$11,664
TOTAL (one-time in Year 1)			**288**		**14,400 hrs.; $1,166,400**	
TOTAL (ongoing in Year 2 and 3)			**4,032**		**47,232 hrs.; $3,825,792**	

The burden hours for the FERC-725B3 information collection are:

Year 1: 14,400 hours
Year 2: 47,232 hours

12 There are 1,414 unique registered entities in the NERC compliance registry as of May 24, 2019. Of this total, we estimate that 288 entities will face an increased paperwork burden due to Docket RD19-3. "Unique registered entities" affected by the Order are Balancing Authority (BA), Distribution Provider (DP), Generator Operator (GOP), Generator Owner (GO), Reliability Coordinator (RC), Transmission Operator (TOP), and Transmission Owner (TO).

13 One-time burdens apply in Year 1 only.

14 R = Requirements

15 Ongoing burdens apply in Year 2 and beyond.

Year 3: 47,232 hours

The total burden hours are 108,864 hours/3 years = 36,288 total burden hours.

The average number of responses for years 1-3 in the FERC-725B3 information collection is:

Year 1: 288
Year 2: 4,032
Year 3: 4,032

The average number of responses/respondents are 8,352/3 years = 2,784 response/respondents on average years 1 to 3.

For submission into ROCIS, the average annual response and burden hour totals for years 1, 2 and 3 are:

Responses: 2,784
Burden Hours: 36,288

The reporting requirements and record keeping requirements are described below:

In the Petition of the North American Electric Reliability Corporation for approval of Proposed Reliability Standard CIP-008-6, dated March 7, 2019, the Standards R1-R4 are:

> **R1.** Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].
>
> **General Considerations for R1**
>
> An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:
>
> Department of Homeland Security, Control Systems Security Program, Developing an
> Industrial Control Systems Cyber Security Incident Response Capability, 2009, online at
> **http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf**

National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61 revision 1, March 2008, online at

http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action.

A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

Implementation Guidance for R1

Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

The figure below is an example of a process that is used to identify, classify and respond to Cyber Security Incidents. This process uses the sample classification schema shown earlier that the entity uses to identify and classify Cyber Security Incidents as well as the sample criteria to evaluate and define attempts to compromise, if they are Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. In this example, the yellow shading is intended to bring emphasis to the steps in this process example where definitions or entity process criteria are met as well as where reporting timelines are triggered. This color scheme is independent from the color keys used in other Figures within this document.

This process is adapted from those related to the Information Technology Infrastructure Library (ITIL). ITIL is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

Note: There is recognition that the organizational structure and resource composition is unique to each entity and that roles and responsibilities may vary. The process diagram to follow is not intended to be prescriptive, and instead constitutes merely one potential approach where the assignments/functions in the

cross functional swim lanes could be tailored to meet the unique needs of any entity.

M1[16]. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*.

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and

Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]

General Considerations for R2

If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."
The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multidiscipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents.

16 M = evidence measure

There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of

evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Implementation Guidance for R2, Acceptable Testing Methods

The SDT made no changes to the testing requirements located in Requirement Parts 2 and 3. The applicable system expansion to include EACMS was the only change. The SDT purposefully did not expand the acceptable testing methods to include an actual response to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. This was based on incident risk level and benefits of exercising the full response plan(s).

Annual testing of the incident response plan(s) are important because they may reveal weaknesses, vulnerabilities, and opportunity for improvement. The current test options include: a paper drill (coordinated tabletop exercise), an operational exercise (a full-scale, multiple entity exercise), and actual response to a Reportable Cyber Security Incident.

Actual response to a Reportable Cyber Security Incident is self-explanatory, whereas the other two types of exercises may carry more subjectivity. To help assure internal organizational alignment, Registered Entities could consider establishing supporting internal definitions for the various types of planned testing. Documentation like this can help participants understand the scope and expectations of those exercises that are not actual response to a Reportable Cyber Security Incident and can aid in the audit process

as a supporting evidence for exercise scenarios. It should be noted that definitions in the NERC Glossary of Terms are authoritative, and entities documenting internal definitions for consistency in their process should assure they do not contradict nor attempt to supersede and authoritative NERC-defined terms. The table below includes some potential ideas that could be used:

Incident Response Exercise – Paper Drill/Tabletop

An activity that is facilitated, where personnel are gathered to discuss various simulated emergency situations including roles, responsibilities, coordination, and

decision making based on the scenario. This typically happens in a conference room or office environment and not in the personnel's normal working environment. No interaction with equipment is expected.

Incident Response Exercise – Operational

An activity that is facilitated, where personnel are gathered to discuss and respond to various simulated emergency situations including roles, responsibilities, coordination, and decision making based on the scenario. This may occur in a test environment or actual operational area. There may be interaction with equipment. The exercise may involve test equipment, actual operational equipment, or training simulators. If operational equipment is used, it will be in a manner as to not jeopardize operational functionality.

All of these options, especially the latter, involve a complete, step-by-step run-through of the plan components. Many problems that would occur in a real incident also will be present in the test exercise or drill**7**. In fact, it is recommended that drills and exercises go to the extreme and simulate worst-case scenarios.

Conversely, a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, may only exercise several components and would likely not result in the same level of response action. Cyber Security Incidents that attempted to compromise an applicable system, by their very nature, have less risk than an actual compromise. A Responsible Entity's actual response to unauthorized access attempts and suspicious activities does not rise to the same level of

required response that actual disruption of a BCS performing one or more reliability tasks would. For these reasons, the SDT did not change the acceptable testing methods of a response plan(s), and using records associated to attempts to compromise are not sufficient evidence to demonstrate compliance with the 15-month testing requirements.

The sample process in Requirement R1.1 shows how an actual Reportable Cyber Security Incident is documented using the entity's incident management system including how each role defined in Requirement R1.3 updates the incident ticket. The incident ticket is a permanent record of the incident including any actions undertaken. The Incident Management Coordinator is responsible for documenting deviations from the Cyber Incident response plan and initiating any corrections required in the process or
documentation for meeting the Requirement. In addition, to assure sufficient evidence, records should be dated and should include documentation that

sufficiently describes the actual or simulated scenario(s), response actions, event identifications and classifications, the application of Cyber Security Incident and

reportability criteria, reportability determinations, and reporting submissions and timeframes.

R2.1. Test each Cyber Security Incident response plan(s) at least once every 15 calendar months:

By responding to an actual Reportable Cyber Security Incident;

With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or

With an operational exercise of a Reportable Cyber Security Incident.

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].

General Considerations for R3

The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a Reportable Cyber Security Incident without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the Reportable Cyber Security Incident.
Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more

time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

Implementation Guidance for R3

The sample process in Requirement R1.1 shows how an actual Reportable Cyber Security Incident results in an update to Cyber Security Incident response plan, incorporating the "lessons learned". The role of Incident Management Coordinator

includes the responsibility for meeting Requirement R3. Registered Entities should assure updated

plans are dated in demonstration of the timelines mandated by Requirement R3. It may help to append these records to the dated Lessons Learned from an actual response or an exercise to test the plan to further demonstrate plan update timelines were met and relevant areas of the plan were updated to align with the outcomes and conclusions in the Lessons Learned.

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1 Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].

General Considerations for R4

Registered Entities may want to consider designing tools or mechanisms to assure incident responders have the information needed to efficiently and timely report events or conditions that rise to the level of reportability. A potential approach is to include the E-ISAC/NCCIC phone numbers in response plans, calling trees, or even within corporate directories for ease of retrieval. Another potential approach is to develop a distribution list that includes both entities so one notification can easily be sent at the same time. Certainly, Registered Entities should consider implementing secure methods for transit if using email. Another approach could be to incorporate website URLs into processes to have them at hand. Finally, for Registered Entities that prefer to leverage secure portals

for E-ISAC or NCCIC, advance planning by having individual user portal accounts requested, authorized, configured, and tested is encouraged ad can be a time saver in emergency situations.

Implementation Guidance for R4

The sample process in Requirement R1.1 shows how initial notification and updates of the required attributes is performed within the specified time lines (yellow colored tasks).
For attributes that are not known, these should be reported as "unknown"

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

Evidence Retention[17]:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

Each Responsible Entity shall retain evidence of each requirement in this standard for three
calendar years.

If a Responsible Entity is found non-compliant, it shall keep information related to the noncompliance 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.

17 Evidence retention is the period of time an entity is required to retain specific evidence to demonstrate compliance.

13. ESTIMATE OF THE TOTAL ANNUAL COST BURDEN TO RESPONDENTS

There are no capital or start-up costs related to this information collection. All costs are related to burden hours.

14. ESTIMATED ANNUALIZED COST TO FEDERAL GOVERNMENT

The estimate of the cost for 'analysis and processing of filings' is based on wages and benefits for professional and clerical support. This estimated cost represents staff analysis, decision-making, and review of any actual filings submitted in response to the information collection.

The Paperwork Reduction Act (PRA) Administrative Cost is the average annual FERC 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. It also includes the cost of publishing the necessary notices in the Federal Register.

	Number of Hours or FTE's	Estimated Annual Federal Cost ($)
PRA[18] Administration Cost[19]	-	$4,931
Data Processing and Analysis[20]	0	$0
FERC Total	-	$4,931

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

The Commission directed NERC to enhance the mandatory reporting of Cyber Security Incidents.[21] The Commission explained that the currently-effective reporting threshold, which only requires reporting in cases where a Cyber Security Incident has "compromised or disrupted one or more reliability tasks," may understate the true scope

18 Paperwork Reduction Act of 1995 (PRA).
19 The PRA Administration Cost is $4,931, and includes preparing supporting statements, notices, and other activities associated with Paperwork Reduction Act compliance.
20 The FY2019 average Commission cost (for wages plus benefits) per FTE (Full-Time Equivalent) is $167,091 (or $80/hour).
21 *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018).

of cyber-related threats to the Bulk-Power System.[22] 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 the Reliability Standard to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).[23] With respect to EACMS, the Commission directed that enhanced reporting should apply, at a minimum, to EACMS that perform the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting.

Reliability Standard CIP-008-6 broadens the mandatory reporting of Cyber Security Incidents and thus addresses the concern that currently-effective Reliability Standard CIP-008-5 may not encompass the full scope of cyber-related threats to the Bulk-Power System.[24] The Reliability Standard will not significantly increase the reporting burden on entities (covered by FERC-725B, which includes the previous version of the standard) because it builds off the currently-effective reporting threshold by expanding it to address reliability gaps, pursuant to section 215(d)(5) of the FPA.

A summary of the burden added to FERC-725B3 information collection due to the Order in RD19-3-000 follows:

FERC-725B3	Total Request	Previously Approved	Change due to Adjustment in Estimate	Change Due to Agency Discretion
Annual Number of Responses	2,784	0	0	2,784
Annual Time Burden	36,288	0	0	36,288
Annual Cost Burden ($)	$0	$0	$0	$0

16. TIME SCHEDULE FOR THE PUBLICATION OF DATA

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

17. DISPLAY OF THE EXPIRATION DATE

22 *Id.* PP 2-3.
23 16 U.S.C. 824o(d)(5) (2012).
24 NERC Petition at 3.

The clearance information and expiration date will be available at http://www.ferc.gov/docs-filing/info-collections.asp.

18. EXCEPTIONS TO THE CERTIFICATION STATEMENT

There are no exceptions.