NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 19, 2019

VIA ELECTRONIC FILING

Mr. Neil Cunningham
Director of Climate Change and Energy Branch
Department of Sustainable Development
1200-155 Carlton Street
Winnipeg MB R3C 3H8

RE: *North American Electric Reliability Corporation*

Dear Mr. Cunningham:

The North American Electric Reliability Corporation ("NERC") hereby submits Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-008-6. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

NERC understands that the Province of Manitoba enacted on April 1, 2012, the Reliability Standards Regulation, which was implemented through an Order of Council. It is NERC's understanding that the Reliability Standards Regulation makes compliance with the NERC reliability standards a legal requirement in Manitoba and adopted the NERC Reliability Standards listed in Schedule 1 of the Regulation for implementation in Manitoba. The Regulation further provides that a reliability standard made by NERC that is listed in Schedule 1 is adopted as a reliability standard for Manitoba.

NERC requests that Manitoba take all necessary action to include Proposed Reliability Standard CIP-008-6 as set forth in the filing in Schedule 1 of the Reliability Standards Regulation, so that it may be adopted as a reliability standard for Manitoba.

Please contact the undersigned if you have any questions concerning this filing.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Respectfully submitted,

/s/ Lauren Perotti

Lauren Perotti
Senior Counsel for the North American Electric Reliability Corporation

Enclosure

BEFORE THE
PROVINCE OF MANITOBA

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-008-6

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

March 19, 2019

TABLE OF CONTENTS

I. SUMMARY 2
II. NOTICES AND COMMUNICATIONS 5
III. BACKGROUND 5
A. NERC Reliability Standards Development Procedure 5
B. Order No. 848 6
C. Development of the Proposed Reliability Standard 7
IV. JUSTIFICATION 8
A. Overview of Proposed Modifications 9
B. Proposed Modifications to NERC Glossary Definitions 11
C. Proposed Modifications to Reliability Standard CIP-008-5 14
D. Enforceability of Proposed Reliability Standard 25
V. EFFECTIVE DATE 26

Exhibit A Proposed Reliability Standard
Exhibit B Implementation Plan
Exhibit C Reliability Standards Criteria
Exhibit D Consideration of Directives
Exhibit E Implementation Guidance
Exhibit F Technical Rationale
Exhibit G Analysis of Violation Risk Factors and Violation Severity Levels
Exhibit H Summary of Development History and Complete Record of Development
Exhibit I Standard Drafting Team Roster

BEFORE THE
PROVINCE OF MANITOBA

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF PROPOSED RELIABILITY STANDARD CIP-008-6

The North American Electric Reliability Corporation ("NERC") hereby submits proposed Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning. The proposed Reliability Standard addresses the Federal Energy Regulatory Commission's ("FERC") directive from Order No. 848[1] to develop modifications to require reporting of Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's[2] Electronic Security Perimeter ("ESP") or associated Electronic Access Control or Monitoring Systems ("EACMS") to the Electricity Information Sharing and Analysis Center ("E-ISAC") and the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT").[3] In addition, the proposed modifications require specific information in Cyber Security Incident reports and include deadlines for submitting the reports as directed by FERC.

The proposed Reliability Standard, provided in Exhibit A hereto, is just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also provides notice of:

---

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

[2] As used in the Critical Infrastructure Protection ("CIP") Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

[3] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, http://www.nerc.com/files/Glossary_of_Terms.pdf ("NERC Glossary").

- the associated Implementation Plan (Exhibit B);
- the proposed revised definitions of Cyber Security Incident and Reportable Cyber Security Incident to be incorporated into the NERC Glossary (Exhibit A);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and G); and
- the retirement of Reliability Standard CIP-008-5.

This filing presents the technical basis and purpose of the proposed Reliability Standard, a summary of the development history (Exhibit H), and a demonstration that the proposed Reliability Standard meets the Reliability Standards criteria (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standard on February 7, 2019.

I. SUMMARY

Proposed Reliability Standard CIP-008-6 requires Responsible Entities to develop and implement Cyber Security Incident response plans. These plans provide a course of action for Responsible Entities to detect incidents that affect BES Cyber Systems,[4] minimize loss and destruction, mitigate weaknesses that were exploited, and help to restore capabilities. The requirements in proposed Reliability Standard CIP-008-6 specify processes and procedures to be included in Cyber Security Incident response plans, implementation and testing of these plans, maintenance of these plans, and mandatory reporting on certain Cyber Security Incidents to facilitate information sharing on threats among relevant entities.

Consistent with Order No. 848, the modifications in proposed Reliability Standard CIP-008-6 broaden the mandatory reporting of Cyber Security Incidents to include compromises or attempts to compromise BES Cyber Systems or their associated ESPs or EACMS. These

[4] The NERC Glossary defines a 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." The acronym BES refers to the Bulk Electric System.

modifications address FERC's concern that the current reporting requirement under CIP-008-5 "may understate the true scope of cyber-related threats facing the Bulk-Power System" insofar as CIP-008-5 only requires reporting of incidents that have actually compromised or disrupted one or more reliability tasks.[5] Consistent with FERC's directive, the proposed standard also: (1) requires certain minimum information be included in the incident reports; (2) includes deadlines for submitting the incident reports; and (3) requires the incident reports to be sent to ICS-CERT, or its successor, in addition to the E-ISAC.[6]

Proposed Reliability Standard CIP-008-6 addresses FERC's directive in Order No. 848 by incorporating each of the above elements within the requirements and relevant definitions in the NERC Glossary, Cyber Security Incident and Reportable Cyber Security Incident, as follows:

- Revisions to Requirement R1 to require:
  - implementing a process that includes criteria to evaluate and define attempts to compromise high and medium impact BES Cyber Systems and their associated ESPs and EACMS; and
  - applying the aforementioned criteria to determine if there was an attempt to compromise applicable systems.
- Revisions to Requirement R2 require:
  - Responsible Entities use their Cyber Security Incident response plans to respond to Cyber Security Incidents that involve attempts to compromise applicable systems; and
  - Responsible Entities retain records related to Cyber Security Incidents that involve attempts to compromise applicable systems.
- Revisions to the Applicable Systems column and NERC Glossary definitions serve to broaden the scope of reporting to include ESPs and EACMS.

Proposed new Requirement R4 requires Responsible Entities to report the following to the E-ISAC and the National Cybersecurity and Communications Integration Center ("NCCIC"), the

5 Order No. 848 at P 2.

6 *Id.* at PP 2-3.

successor to ICS-CERT[7]: (1) Reportable Cyber Security Incidents, which are proposed to include Cyber Security Incidents that have compromised or disrupted ESPs, EACMS, or a BES Cyber System that performs one or more reliability tasks of a functional entity; and (2) attempts to compromise a BES Cyber System, an ESP, or an EACMS, as defined by the Responsible Entity's criteria. These initial reports must occur within the following timelines: (1) one hour of the Responsible Entity's determination of a Reportable Cyber Security Incident and (2) by the end of the next calendar day after determination of an attempt to compromise a BES Cyber System, an ESP, or an EACMS. If known at the time of initial notification, Responsible Entities must report on the following three attributes: (1) the functional impact, (2) the attack vector used, and (3) the level of intrusion that was achieved or attempted. If not reported during initial notification, Responsible Entities must report on the each of the three attributes within seven days of the determination of each attribute.

By broadening the reporting requirements, the proposed modifications are expected to enhance awareness of existing and future cyber security threats and potential vulnerabilities. The proposed standard provides Responsible Entities the flexibility to assess the unique characteristics of their operating environment and identify and report suspicious activities accordingly. By allowing Responsible Entities the flexibility to refine their reporting, the E-ISAC and the NCCIC can expect to receive more accurate information on actual threats. The resulting information sharing from enhanced reporting to the E-ISAC and the NCCIC will help to better prepare the electric industry to protect critical infrastructure against compromise.

[7] Since Order No. 848 was issued, ICS-CERT functions have been taken over by NCCIC. As such, the standard drafting team used NCCIC, the successor of ICS-CERT, in its proposed revisions. In addition, the standard drafting team included "or their successors" after the E-ISAC and NCCIC to help ensure the standard stays relevant if either organization changes its name or its duties fall to another organization in the future.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Howard Gugel
Senior Director of Engineering and Standards
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
howard.gugel@nerc.net

III. BACKGROUND

The following background information is provided below: (a) a description of the NERC Reliability Standards Development Procedure; (b) an overview of the Order No. 848 directive addressed in this filing; and (c) the history of the Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting.

A. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Reliability Standard development process. NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[8] NERC's rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfy certain criteria for approving Reliability

[8] The NERC Rules of Procedure are available at: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the Board is required before NERC submits the Reliability Standard to the applicable governmental authorities.

B. Order No. 848

Order No. 848 adopts the proposals included in a Notice of Proposed Rulemaking issued by FERC on December 21, 2017.[9] In Order No. 848, FERC directed NERC to develop and submit modifications to the NERC Reliability Standards to augment mandatory reporting of Cyber Security Incidents.[10] FERC directed the modifications to be submitted to FERC within six months of the effective date of Order No. 848.[11] Specifically, FERC directed that NERC modify the standard to:

- expand mandatory reporting of Cyber Security Incidents to include compromises of, or attempts to compromise, a Responsible Entity's ESP and associated EACMS performing certain functions;
- require certain attributes in the incident reports;
- include timelines for submitting the incident reports based on the severity of the incident; and
- require incident reports be submitted to the ICS-CERT, or its successor, in addition to the E-ISAC.

FERC also directed NERC to submit an annual anonymized, public summary of the reports to FERC.[12]

---

[9] Notice of Proposed Rulemaking, *Cyber Security Incident Reporting Reliability Standards*, 161 FERC ¶ 61,291 (2017).

[10] Order No. 848 at P 16.

[11] *Id.* at P 37.

[12] Order No. 848 at P 16.

As mentioned above, FERC directed that NERC require that the incident reports include the following minimum set of attributes: "(1) the functional impact, where possible, 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."[13] FERC also directed NERC to develop reporting timelines that consider the severity of the event and the risk to BES reliability.[14]

FERC also provided guidance on certain aspects of how NERC should identify EACMS for reporting purposes and define "attempts to compromise." With regard to EACMS, FERC stated that NERC's reporting threshold should encompass the functions that various EACMS technologies provide, which must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting.[15] With regard to the definition of "attempted compromise" for reporting purposes, FERC stated it "considers attempted compromise to include an unauthorized access attempt or other confirmed suspicious activity."[16]

C. Development of the Proposed Reliability Standard

As further described in Exhibit H hereto, NERC initiated Project 2018-02 Modifications to CIP-008 ("Project 2018-02") and appointed a standard drafting team (Exhibit I) to address FERC's directive in Order No. 848. On October 3, 2018, NERC posted the initial draft of proposed Reliability Standard CIP-008-6 for a 20-day comment period, which included an initial ballot

---

13 *Id*. at P 91.

14 *Id*. at P 89.

15 *Id*. at P 54.

16 *Id*. at P 55.

during the last 5 days of the comment period.[17] The initial ballot did not receive the requisite approval from the ballot pool. After considering comments to the initial draft, NERC posted a second draft of CIP-008-6 for a 15-day comment period and ballot on November 15, 2018, which included an additional ballot during the last 10 days of the comment period.[18] The second draft of proposed Reliability Standard CIP-008-6 received the requisite approval with affirmative votes of 75.54 percent of the ballot pool. On January 15, 2019, NERC conducted an eight-day final ballot for proposed Reliability Standard CIP-008-6, which received affirmative votes of 77.89 percent of the ballot pool.[19] The Board adopted the proposed Reliability Standard on February 7, 2019.

IV. JUSTIFICATION

As discussed below and in Exhibit C, the proposed Reliability Standard addresses FERC's directive in Order No. 848 to broaden mandatory reporting requirements and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. This section provides an explanation of the following:

- Overview of proposed modifications (Subsection A);
- Proposed modifications to NERC Glossary definitions (Subsection B);
- Proposed modifications to the CIP-008-5 Reliability Standard (Subsection C); and
- The enforceability of the proposed Reliability Standard (Subsection D).

[17] Pursuant to Standard Processes Manual Section 16, the NERC Standards Committee granted NERC's request to waive Standard Processes Manual provisions 4.7-4.9 to post the Reliability Standard for a 45-day initial comment period and ballot.

[18] Pursuant to Standard Processes Manual Section 16, the NERC Standards Committee granted NERC's request to waive Standard Processes Manual provisions 4.9 and 4.12 to post the Reliability Standard for a 45-day additional comment period and ballot.

[19] Pursuant to Standard Processes Manual Section 16, the NERC Standards Committee granted NERC's request to waive Standard Processes Manual provision 4.9 to post the Reliability Standard for a 10-day final ballot.

A. Overview of Proposed Modifications

The purpose of currently effective Reliability Standard CIP-008-5 is to mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Reliability Standard CIP-008-5 advances this objective by requiring the following:

- implementing a Cyber Security Incident response plan that includes:
  - processes to identify, classify, and respond to Cyber Security Incidents;
  - processes to determine whether a Cyber Security Incident should be reported to the E-ISAC as a Reportable Cyber Security Incident within one hour of determination;
  - roles and responsibilities of Cyber Security Incident response groups or individuals; and
  - incident handling procedures for Cyber Security Incidents;
- testing and using the Cyber Security Incident response plan and retaining records related to Reportable Cyber Security Incidents; and
- maintaining the plan based on testing or actual Reportable Cyber Security Incidents or based on changes to roles, responsibilities, individuals, groups, or technology.

Similar to Reliability Standard CIP-008-5, proposed Reliability Standard CIP-008-6 advances the same objective through expanded mandatory reporting requirements. Currently under CIP-008-5, incidents that meet the definition of Cyber Security Incident are subject to the Cyber Security Incident response plan. Under Reliability Standard CIP-008-5, only Cyber Security Incidents that meet the definition of Reportable Cyber Security Incident are those that are subject to reporting requirements pursuant to Requirement R1, Part 1.2. As part of this broadening of the reporting requirements, proposed CIP-008-6 expanded the NERC Glossary definition of Reportable Cyber Security Incident as well as Cyber Security Incident to capture additional incidents.

Moreover, there are more Cyber Security Incidents to report under proposed CIP-008-6 than those included as a Reportable Cyber Security Incident. Proposed CIP-008-6, Requirement

R4 also requires Responsible Entities to report Cyber Security Incidents that meet the criteria for attempts to compromise applicable systems as defined under Requirement R1, Part 1.2. Because attempts to compromise applicable systems will be defined by each Responsible Entity, the standard drafting team determined that it is appropriate to include that obligation in the requirement language rather than have a NERC Glossary definition that requires Responsible Entities to develop a definition. As a result, under the proposed Reliability Standard CIP-008-6, Responsible Entities are required to report more Cyber Security Incidents than only those that meet the definition of Reportable Cyber Security Incident. Although proposed Reliability Standard CIP-008-6 retains much of the structure of CIP-008-5, this is a change from the current obligation to only report those Cyber Security Incidents that meet the Reportable Cyber Security Incident definition.

Incident reports for both Reportable Cyber Security Incidents and Cyber Security Incidents that are attempts to compromise applicable systems must contain the following attributes, either initially or as a follow up: (1) the functional impact; (2) the attack vector used; and (3) the level of intrusion that was achieved or attempted as required under proposed Requirement R4, Part 4.1.

Proposed CIP-008-6, Requirement R4, Parts 4.2 and 4.3 include timelines for initial reports as well as follow up reports to the E-ISAC and NCCIC. Initial reports for Reportable Cyber Security Incidents must occur within one hour of its determination. Once a Responsible Entity has determined that a Cyber Security Incident meets its criteria for an attempt to compromise an applicable system, it must report the Cyber Security Incident by the end of the next calendar day. Finally, if the Responsible Entity did not include one or more of the attributes in its initial report as it was unknown at the time, it must report the attributes within seven days of determining the attribute.

As described more fully in Sections B and C, proposed Reliability Standard CIP-008-6 addresses the components of the directive throughout proposed Requirements R1, R2, and R4; the revised Applicable Systems column for all requirements; and the revised definitions as follows:

- Report to NCCIC: Requirement R4 addresses the component to send reports to NCCIC in addition to E-ISAC.
- Attempts to compromise: Revisions to Requirement R1, Part 1.2 and Requirement R2, Parts 2.2 and 2.3 and new Requirement R4 address the component on defining attempts to compromise applicable systems and reporting on Cyber Security Incidents that are attempts to compromise applicable systems.
- EACMS and ESP: The revised Applicable Systems column and the revisions to the definitions address the component on adding compromises and attempts to compromise EACMS and ESP to those Cyber Security Incidents that must be reported.
- Attributes: Requirement R4, Part 4.1 addresses the component of the directive requiring certain content, or attributes, to be included in reports.
- Timelines: Requirement R4, Parts 4.2 and 4.3 address the component in the directive on timelines for initial and follow up reporting.

B. Proposed Modifications to NERC Glossary Definitions

The Project 2018-02 standard drafting team revised two definitions in the NERC Glossary to address the Order No. 848 directive: Cyber Security Incident and Reportable Cyber Security Incident. The following sections describe how the revisions to each definition address the directive.

1) Cyber Security Incident

NERC proposes to revise the definition of Cyber Security Incident as follows:

A malicious act or suspicious event that:

- **For a high or medium impact BES Cyber System, C**~~**c**~~ompromises~~,~~ or ~~was an~~ attempt**s** to compromise~~,~~ **(1)** ~~the~~ **an** Electronic Security Perimeter**,** ~~or~~**(2) a** Physical Security Perimeter**,** or~~,~~ **(3) an Electronic Access Control or Monitoring System; or**
- Disrupts~~,~~ or ~~was an~~ attempt**s** to disrupt~~,~~ the operation of a BES Cyber System.

The definition of Cyber Security Incident is foundational for proposed CIP-008-6. Once a Responsible Entity determines that an event is a Cyber Security Incident, the Responsible Entity

must comply with the requirements of proposed Reliability Standard CIP-008-6, including initiating its response plan and reporting the incident to the E-ISAC and the NCCIC, if applicable.

As discussed above, FERC directed NERC to require reporting of compromises and attempts to compromise EACMS, particularly those that perform: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting. To address the directive, the standard drafting team revised the definition of Cyber Security Incident to include compromises or attempts to compromise EACMS. The standard drafting team observed that nearly all EACMS perform at least one of the functions listed by FERC. As a result, the standard drafting team included all EACMS in the Cyber Security Incident definition rather than list the functions. This meets the intent of FERC's directive while providing a clear and concise definition.

The revised definition of Cyber Security Incident also includes revisions that improve clarity. First, the definition clarifies that compromises or attempts to compromise an ESP, PSP, or EACMS are for high or medium impact BES Cyber Systems. The current definition of Cyber Security Incident does not include the phrase "for high or medium impact BES Cyber Systems" when referring to ESP and PSP. However, under the CIP suite of standards, only high and medium impact BES Cyber Systems have ESPs and PSPs. Adding the phrase "for high or medium impact BES Cyber Systems" clarifies the intent of the definition. Second, the standard drafting team revised the definition for verb agreement. The standard drafting team changed "was an attempt" to "attempts" so that the verb agrees with the tense of "compromises." These changes enhance the Cyber Security Incident definition by providing additional clarity.

2) Reportable Cyber Security Incident

The standard drafting team determined to include only actual compromises or disruptions, not attempts to compromise, in the definition of Reportable Cyber Security Incident, while the proposed requirements require reporting of attempts to compromise applicable systems, as discussed more fully in Section C. As noted previously, this means the definition of Reportable Cyber Security Incident does not include all those Cyber Security Incidents that must be reported under the proposed standard.

NERC proposes to revise the definition of Reportable Cyber Security Incident as follows:

A Cyber Security Incident that ~~has~~ compromised or disrupted**:**

- **A BES Cyber System that performs** one or more reliability tasks of a functional entity~~.~~**;**
- **An Electronic Security Perimeter of a high or medium impact BES Cyber System; or**
- **An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.**

To meet the component of the FERC directive regarding ESP and EACMS, the standard drafting team added compromises of ESP and EACMS to the Reportable Cyber Security Incident definition. In doing so, these types of Cyber Security Incidents become Reportable Cyber Security Incidents, which broadens the reporting requirements consistent with the directive in Order No. 848.

Revisions to the Reportable Cyber Security Incident definition further broaden the reporting requirements to include compromises or disruptions of a BES Cyber System that performs one or more reliability tasks of a functional entity. Under the current definition, a Reportable Cyber Security Incident only includes a compromise or disruption of the reliability tasks. By adding the phrase "[a] BES Cyber System that performs," Responsible Entities will be required to report on a compromise of a BES Cyber System even if it has not affected performance

of that BES Cyber System's tasks. This helps to ensure that Responsible Entities report on, for example, malware installed on a BES Cyber Asset part of a BES Cyber System that performs one or more reliability tasks regardless of whether the BES Cyber System still operates.

Finally, similar to clarifications to the Cyber Security Incident definition, the standard drafting team qualified ESP and EACMS with "of a high or medium impact BES Cyber System" and changed the tense of the verbs "compromised or disrupted" from past perfect to past tense.

C. Proposed Modifications to Reliability Standard CIP-008-5

This section discusses the modifications in proposed Reliability Standard CIP-008-6 and how they address FERC's Order No. 848 directive, as follows:

- Subsection 1 describes revisions to the Applicable Systems column in the table of proposed Reliability Standard CIP-008-6 for Requirements R1, R2, R3, and R4 and how these revisions address the component of the directive to report compromises and attempts to compromise EACMS.
- Subsection 2 provides detail on proposed Requirement R1, and how the revisions address the component of the directive on attempts to compromise applicable systems.
- Subsection 3 provides detail on proposed Requirement R2, and how the revisions address the component of the directive on attempts to compromise applicable systems.
- Subsection 4 describes proposed new Requirement R4 and how it addresses the following components of the Order No. 848 directive: 1) reporting to NCCIC; 2) reporting on attempts to compromise applicable systems; 3) attributes to be reported; and 4) timelines for reporting.
- Subsection 5 highlights other minor modifications in proposed Reliability Standard CIP-008-6.

1) Applicable Systems Column

As noted in the Background section of proposed CIP-008-6, "[e]ach table [in the requirements in the CIP suite of standards] has an 'Applicable Systems' column to further define the scope of systems to which a specific requirement row applies. The [standard drafting team for CIP-008-5] adapted this concept from the National Institute of Standards and Technology Risk

Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics."[20]

The Applicable Systems column in the tables for Requirements R1, R2, R3, and R4 are revised to include EACMS associated with high and medium impact BES Cyber Systems to bring those systems within the scope of the CIP-008-6 requirements. Proposed Reliability Standard CIP-008-6 does not distinguish between different types of EACMS with respect to applicability as nearly all EACMS perform at least one of the five functions identified by FERC in Order No. 848 (i.e., authentication, monitoring and logging, access control, Interactive Remote Access, and alerting).[21]

As ESPs are not "systems," they are not specifically listed in the Applicable Systems column of the tables. However, compromises and attempts to compromise ESPs are within the scope of the proposed standard and must be reported. Under the proposed standard, a Responsible Entity must consider whether a Cyber Security Incident involved compromises or attempts to compromise high or medium impact BES Cyber Systems. Under Reliability Standard CIP-005-5, those BES Cyber Systems, if connected to a network via a routable protocol, must reside within ESPs. In attempting to compromise an ESP, an attacker is attempting to compromise a high or medium impact BES Cyber System. Moreover, the Electronic Access Point[22] ("EAP") on the ESP can be considered an EACMS. Any attempts on the EAP would be brought into scope based on

---

[20] *See* Exhibit A to this filing, Background section of proposed CIP-008-6 at 4; information on the National Institute of Standards and Technology Risk Management Framework is available at https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview.

[21] Order No. 848 at P 54.

[22] The NERC Glossary defines the EAP as, "[a] Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter." Under CIP-005-5, Requirement R1, Part 1.2, all External Routable Connectivity for applicable systems must be through an identified EAP.

the EACMS in the Applicable Systems column. As a result, ESP is automatically brought into scope of the proposed Reliability Standard CIP-008-6 reporting requirements by virtue of the inclusion of medium and high impact BES Cyber Systems and EACMS in the Applicable Systems column without need for a specific reference.

2) Requirement R1

The revisions to proposed Requirement R1 include the following:

- Adding processes that include criteria to evaluate and define attempts to compromise applicable systems;[23]
- Adding processes to identify Cyber Security Incidents that are attempts to compromise applicable systems; and
- Adding that the processes to provide notification are per Requirement R4.

Requirement R1, Part 1.2 is expanded to include the following requirements to be applied to high and medium impact BES Cyber Systems and their associated EACMS, as follows:

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include…

1.2 One or more processes ~~to~~**:**

1.2.1 **That include criteria to evaluate and define attempts to compromise;**

1.2.2 **To** determine if an identified Cyber Security Incident is ~~a~~**:**

- **A** Reportable Cyber Security Incident ~~and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.~~**; or**
- **An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and**

1.2.3 **To provide notification per Requirement R4.** ~~Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.~~[24]

[23] Applicable systems refers to high and medium impact BES Cyber Systems and their associated EACMS.

[24] This language is an excerpt from Requirement R1 and only includes language relevant to understanding the proposed revisions.

Proposed Requirement R1, Parts 1.2.1 and 1.2.2 address one component of the directive from Order No. 848 to broaden reporting on Cyber Security Incidents to include those that "attempt to compromise" an ESP or EACMS. In proposed Requirement R1, Part 1.2.1, each Responsible Entity must develop a process that includes criteria to evaluate and define attempts to compromise applicable systems. Proposed Requirement R1, Part 1.2.2 requires that each Responsible Entity develop a process that identifies whether a Cyber Security Incident is an "attempt to compromise" pursuant to the criteria required by Part 1.2.1. Parts 1.2.1 and 1.2.2 work together to help ensure each Responsible Entity first develops criteria for an attempt to compromise then applies the criteria during its Cyber Security Incident identification process.

Based on standard drafting team discussion and subject matter expert comments, the standard drafting team determined that the best approach for promoting meaningful and accurate reporting would be for each Responsible Entity to develop its own criteria to determine which Cyber Security Incidents amount to an "attempt to compromise" a BES Cyber System, ESP, or EACMS. This criteria indicates what types of Cyber Security Incidents must then be reported to the E-ISAC and NCCIC. Each Responsible Entity has a unique operational environment that experiences different threats. For example, an entity with an EACMS containing both an EAP and a corporate facing interface to its business networks is likely to experience significantly more traffic than an entity with a system architecture involving security zones or network segmentation. As such, the first entity would likely not view the same level of traffic as suspicious compared to the second entity. Proposed Parts 1.2.1 and 1.2.2 recognize differences in system architecture and provide each Responsible Entity with the flexibility to develop criteria that reflect what it considers

"suspicious." The benefit of such an approach, compared to a one-size-fits-all approach, is that it would enable Responsible Entities to better capture real attempts to compromise.[25]

As noted in previous filings on CIP standards, the ERO has the authority to evaluate the reasonableness of the Responsible Entity's criteria when assessing compliance to ensure the criteria meets the reliability objective of CIP-008-6.[26] This is consistent with NERC's statutory obligation to engage in meaningful compliance oversight and consistent with its oversight of other CIP standards where Responsible Entities are afforded discretion.[27]

3) Requirement R2

Proposed Requirement R2, which requires the implementation and testing of Cyber Security Incident response plans, is revised to add attempts to compromise applicable systems in the required processes developed under Requirement R1 (Requirement R2, Part 2.2) and the record retention obligations (Requirement R2, Part 2.3). These revisions are incorporated into proposed Requirement R2, Parts 2.2 and 2.3, which include the following requirements to be applied to high and medium impact BES Cyber Systems and their associated EACMS:

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include…

2.2 Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident**, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part,** or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.

---

[25] As an example of how to develop and apply criteria, the standard drafting team developed a proposed implementation guidance, included in this filing as Exhibit E.

[26] *Notice of Filing of the North American Electric Reliability Corporation of Proposed Reliability Standard CIP-003-7*, at 20-22, (Mar. 10, 2017).

[27] There is language in the following CIP standards requirements granting Responsible Entities a degree of discretion: CIP-003-7, Section 3.1; CIP-004-6, Requirement R4, Parts 4.1, 4.3, and 4.4, Requirement R5, Parts 5.2 and 5.5; CIP-007-6, Requirement R1, Part 1.1 and Requirement R4, Parts 4.2 and 4.4; CIP-008-5, Requirement R3, Part 3.2; and CIP-009-6, Requirement R3, Part 3.2.

2.3 Retain records related to Reportable Cyber Security Incidents **and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1**.[28]

Similar to the revisions in Requirement R1, the revisions to Requirement R2 address the component of FERC's directive regarding attempts to compromise. The revisions to Part 2.2 serve to reinforce that Responsible Entities must use their Cyber Security Incident response plans when responding to a Cyber Security Incident determined to be an attempt to compromise applicable systems. The revisions to Part 2.3 require Responsible Entities to retain records related to these types of Cyber Security Incidents.

4) Requirement R4

Proposed Requirement R4 is a new requirement, applicable to high and medium impact BES Cyber Systems and their associated EACMS. It includes requirements to report certain Cyber Security Incidents to the E-ISAC and the NCCIC. Proposed Requirement R4 also specifies the (1) required content, or attributes, in those incident reports; and (2) timeframes for initially reporting the incident and updating the initial report with additional information, as follows:

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),[29] 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

[28] This language is an excerpt from Requirement R2 and only includes language relevant to understanding the proposed revisions.

[29] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

by law, in accordance with each of the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*.

4.1 Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:
- **4.1.1** The functional impact;
- **4.1.2** The attack vector used; and
- **4.1.3** The level of intrusion that was achieved or attempted.

4.2 After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:
- One hour after the determination of a Reportable Cyber Security Incident.
- By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.

4.3 Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.

Proposed Requirement R4 addresses FERC's directive to require that each report and update must be sent to the E-ISAC and NCCIC. Currently, Reliability Standard CIP-008-5, Requirement R1, Part 1.2 requires Responsible Entities to send notification of Reportable Cyber Security Incidents within an hour of determination to the E-ISAC. The standard drafting team retained this requirement, moving it into Requirement R4, and broadened the reporting requirements to include NCCIC as a receiving entity for notification and any follow-up reports. These notifications and updates must come directly from the Responsible Entity to each agency.

In Order No. 848, FERC directed NERC to revise Reliability Standard CIP-008-5 to require Responsible Entities to submit reports directly to both the E-ISAC and ICS-CERT, or its successor (now NCCIC). Requirement R4 thus achieves the benefits listed in Order No. 848 of helping to ensure timely analysis and notification to other entities of cyber threats and the protection of confidential information by requiring Responsible Entities report directly to each organization.[30]

[30] Order No. 848 at P 90.

Proposed Requirement R4 also requires that Responsible Entities report Cyber Security Incidents that are attempts to compromise applicable systems. Proposed Requirement R4 includes a reference to an attempt to compromise, as determined by applying the criteria from Part 1.2.1, to indicate that the Responsible Entity's criteria defines what should be reported as an attempt to compromise. In addition, proposed Requirement R4, Part 4.2 references the determination made pursuant to Part 1.2 to indicate that a Cyber Security Incident identified as an attempt to compromise based on the Responsible Entity's identification must be reported by the end of the next calendar day, as discussed more fully below.

Requirement R4, Part 4.1 includes the list of attributes a Responsible Entity must submit to E-ISAC and NCCIC. The standard drafting team incorporated the attributes directed by FERC in Order No. 848 as required to be reported to E-ISAC and NCCIC: (1) the functional impact; (2) the attack vector used; and (3) the level of intrusion that was achieved or attempted.

Each Responsible Entity must report all information on the attributes known at the time of reporting pursuant to proposed Part 4.1. However, a Responsible Entity must still submit an initial report even if upon initial notification the Responsible Entity does not have information on attributes. The Responsible Entity must then follow up with E-ISAC and NCCIC within the timeline prescribed by proposed Part 4.3 once attributes are known. The proposed provision thus strikes a necessary balance between the need to report compromises and attempts to compromise in a timely manner with the need to perform thorough, accurate, and complete investigations into Cyber Security Incidents.

Proposed Requirement R4 also dictates timelines for reporting in response to Order No. 848. Proposed Requirement R4, Part 4.2 requires Responsible Entities to notify the E-ISAC of Reportable Cyber Security Incidents within one hour, which is currently required in Reliability

Standard CIP-008-5, Requirement R1, Part 1.2. This one hour notification timeline also applies to reports to NCCIC on Reportable Cyber Security Incidents, consistent with Order No. 848. For attempts to compromise a BES Cyber System, ESP, or EACMS, proposed Part 4.2 requires notification to both E-ISAC and NCCIC by the end of the next calendar day after determination that the Cyber Security Incident was an attempt to compromise.

The proposed notification timelines appropriately reflect the severity of the risk of the respective incidents. Order No. 848 directed that NERC should, "establish reporting timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."[31] In an actual compromise of an applicable system, the potential risk of a BES Cyber System impacting reliability is high. As such, proposed CIP-008-6 would require an entity to report such an incident within one hour of determining that the incident was a compromise. Such prompt information sharing allows Responsible Entities to take action to protect BES reliability from the impacts of the loss or misuse of that compromised BES Cyber System.

For attempts to compromise an applicable system, the risk of impact to BES reliability is lower because the attacker did not successfully infiltrate the applicable system. Sharing information on such attempts to compromise helps broaden entities' situational awareness, but it does not require the same type of urgent response required after an applicable system is compromised. Accordingly, under proposed CIP-008-6 Requirement R4, Part 4.2, the Responsible Entity would have a longer period to report than that provided for an actual compromise. Specifically, the Responsible Entity would be required to report such attempted compromises by the end of the next calendar day. This reporting timeline is appropriate to reflect the severity and

[31] *Id*. at P 89.

risk of these unsuccessful attacks. Further, this reporting timeline provides clarity and provides for consistent application of requirement language.

In drafting the proposed requirement, the standard drafting team considered FERC's guidance in Order No. 848 that, "[f]or lower risk incidents, such as the detection of attempts at unauthorized access to the responsible entity's ESP or associated EACMS, an initial reporting timeframe between eight and twenty-four hours would provide an early indication of potential cyber attacks."[32] While recognizing the need for prompt reporting of such incidents, the standard drafting team determined that such an hours-based approach could result in entities needing to track arbitrary deadlines. For example, if the Responsible Entity makes its determination at 4:39 p.m. on day one, then the deadline to report would be 24 hours later at 4:39 p.m. on day two. Using 24 hours as a deadline would make the Responsible Entity have to keep track of an arbitrary deadline every time the Responsible Entity needed to report an attempt to compromise. The benefit of requiring an entity to report by the end of the next calendar day is that it provides a consistent deadline, 11:59 p.m. local time on day two, for each Cyber Security Incident that needs to be reported as an attempt to compromise. Responsible Entities can then focus their efforts on investigating the details of the Cyber Security Incident and submitting accurate and timely reports.

For clarity, and to maintain consistency with the current standard, both reporting deadlines are triggered from the determination that a Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise. This determination is based on each Responsible Entity's process for identification as required under Requirement R1, Part 1.2 of both Reliability Standard CIP-008-5 and proposed Reliability Standard CIP-008-6. Arriving at this determination often takes some investigation, and triggering the timeline from the result of this determination provides the

[32] *Id*.

most clarity in requirement language and is consistent with language from Reliability Standard CIP-008-5.

In addition, the standard drafting team added a seven-day timeframe for submitting updated information on any unreported attributes from Part 4.1. The seven-day timeline to report starts when the Responsible Entity determines the attribute. The seven-day timeline does not start from the initial notification of the Cyber Security Incident. Similar to the other notification timeframes in Part 4.2, the notification timeline in Part 4.3 is triggered by the Responsible Entity's process. This allows the Responsible Entity to conduct an appropriate investigation that provides timely notification to the relevant organizations but is not rushed by arbitrary deadlines. Further, it helps to ensure a thorough investigation and more accurate information sharing so that the true threat, or extent of intrusion, is reported.

5) Other Modifications

Proposed Reliability Standard CIP-008-6 also contains a number of minor modifications to align the standard with revisions to other standards or initiatives in other areas.

First, the Interchange Coordinator or Interchange Authority is removed from the Applicability section of proposed Reliability Standard CIP-008-6. This revision is consistent with changes to the NERC Compliance Registry under the risk-based registration initiative.[33]

[33] *Notice of Filing of the North American Electric Reliability Corporation of Risk-Based Registration Initiative Rules of Procedure Revisions, filed on January 6,* 2015 (proving notice of removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

Second, the term "Special Protection Systems" in Applicability subsections 4.1.2.2 and 4.2.1.2 has been replaced with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[34]

Finally, while not a mandatory and enforceable part of the standard, the Guidelines and Technical Basis section has been removed from proposed Reliability Standard CIP-008-6 consistent with changes in how NERC maintains such material.[35]

D. Enforceability of Proposed Reliability Standard

The proposed Reliability Standard also includes Measures that support the requirements by clearly identifying what is required and how the ERO will enforce the requirements. The Measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party. Additionally, the proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirement of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and FERC guidelines related to their assignment. Exhibit G provides a detailed review of the revised VRF and VSLs, and the analysis of how the VRF and VSLs were determined using these guidelines.

---

[34] On February 25, 2015, NERC submitted a notice of a revised definition of the term "Remedial Action Scheme" and certain proposed Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes". *Notice of Filing of the North American Electric Reliability Corporation of Revisions to the Definitionof "Remidial Action Scheme" and Proposed Reliability Standards,* February 25, 2015.

[35] Consistent with NERC's Compliance Guidance Policy, the information formerly in this section is now in proposed implementation guidance (Exhibit E) and a technical rationale document (Exhibit F). For more information, please refer to the NERC Compliance Guidance Policy available at: https://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf.

V. EFFECTIVE DATE

As provided in Exhibit B hereto, the proposed Implementation Plan provides that, where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction. As to the proposed modified definitions, the Implementation Plan provides, where approval by an applicable governmental authority is required, the definition shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-008-6, or as otherwise provided for by the applicable governmental authority. Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date that Reliability Standard CIP-008-6 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

The 18-month implementation period is designed to afford Responsible Entities sufficient time to ensure entities can be fully compliant with the proposed Reliability Standard by the effective date. The proposed implementation period reflects considerations provided by subject matter experts that eighteen months is needed to provide Responsible Entities time to develop and implement Cyber Security Incident response plans that incorporate the broadened reporting

requirements. In addition, NERC and E-ISAC may use this time to consider how to appropriately collect the potential increase in the number of reports.

Eighteen months provides entities the necessary time to develop the criteria for defining attempts to compromise. As noted above, proposed Requirement R1, Part 1.2 requires entities to have a process that includes criteria for defining attempts to compromise. Subject matter experts indicated that development of this criteria will take resources to help ensure that the criteria set the appropriate thresholds to capture actual attempts to compromise. Without the proper time to consider this criteria, entities risk either capturing too much or too little of what should be reported. The former may inundate the entity, E-ISAC, and NCCIC with unnecessary and unhelpful information, whereas the latter would not alert industry to potential risks. As such, entities need time to carefully consider appropriate criteria and train on this criteria so that staff can apply it correctly.

In addition, the proposed 18-month implementation period helps entities maintain their existing schedule for testing of Cyber Security Incident response plans as currently required under Requirement R2, Part 2.1 of CIP-008-5. In that requirement, entities must test their Cyber Security Response Plans at least once every 15 calendar months. Proposed CIP-008-6 retains this requirement. With an 18-month implementation period, entities can incorporate the updated requirements into their existing testing schedule rather than reset their schedule solely for compliance purposes.

Finally, subject matter experts commented that obtaining approval for cost increases within their entities' annual budget cycle impacts how quickly an entity can implement enhanced requirements. For smaller entities, enhanced requirements may require extra consulting services to implement the requirements or to provide cyber security expertise. In addition, entities may

need to hire new staff or install new equipment, such as enhanced logging capabilities, to implement the requirements. Each of these items needs budget approval, and depending on the timing of the annual budget cycle, some entities may not get approval until nearly a year after issuance of an order or other actions approving proposed CIP-008-6. As such, these entities would need additional time after the budget approval to actually implement CIP-008-6. The standard drafting team determined that 18 months provided time for entities to secure necessary funding within the annual budget cycle and to implement the requirements prior to the effective date of CIP-008-6.

Respectfully submitted,

/s/ Marisa Hecht
Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: March 19, 2019

EXHIBITS A - B and D - I

EXHIBIT C

Reliability Standards Criteria

The discussion below explains how the proposed Reliability Standard meets or exceeds the Reliability Standards criteria.

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.

The proposed Reliability Standard improves upon and expands information sharing required by NERC's CIP Reliability Standards by requiring Responsible Entities to report on 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") to the Electricity Information Sharing and Analysis Center ("E-ISAC") and the National Cybersecurity and Communications Integration Center ("NCCIC"), consistent with the FERC directive in Order No. 848.[1] Specifically, proposed Reliability Standard CIP-008-6 improves reliability by requiring Responsible Entities to report Reportable Cyber Security Incidents to E-ISAC and NCCIC within one hour of the determination of the incident and to report Cyber Security Incidents by the end of the next calendar day after determination that the Cyber Security Incident was an attempt to compromise a BES Cyber System, ESP, or EACMS. The reports must include the following three attributes: (1) the functional impact; (2) the attack vector used; and (3) the level of intrusion that was achieved or attempted. If a Responsible Entity does not have this information within the initial reporting timeframe, the Responsible Entity must report the information once it has been determined within seven days of that determination. Exhibit F

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

includes technical rationale for the proposed Reliability Standard to demonstrate the technical soundness of the means to achieve the reliability goal.

2. **Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.**

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply. The proposed Reliability Standard applies to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standard clearly articulates the actions that such entities must take to comply with the standard.

3. **A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.**

The Violation Risk Factors and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and FERC guidelines related to their assignment, as discussed further in Exhibit G. The assignment of the severity level for each VSL is consistent with the corresponding requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences.

4. **A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner.**

The proposed Reliability Standard contains measures that support the requirements by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirements will be enforced and help ensure that the

requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

5. **Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.**

The proposed Reliability Standard achieves the reliability goals effectively and efficiently. The proposed Reliability Standard clearly articulates the security objective that applicable entities must meet and provides entities the flexibility to tailor their plan(s) required under the standard to best suit the needs of their organization.

6. **Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.**

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. The proposed Reliability Standard satisfies FERC's directive in Order No. 848.

7. **Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.**

The proposed Reliability Standard applies throughout North America and does not favor one geographic area or regional model.

8. **Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.**

The proposed Reliability Standard has no undue negative impact on competition. The proposed Reliability Standard requires the same performance by each of the applicable

Functional Entities. The proposed Reliability Standard does not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.

The proposed 18-month implementation period for the proposed Reliability Standard is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop and implement the necessary plans and processes, conduct any training, and continue on their schedule for testing Cyber Security Plans at least once every 15 calendar months.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Reliability Standard development process.

The proposed Reliability Standard was developed in accordance with NERC's ANSI-accredited processes for developing and approving Reliability Standards. Exhibit H includes a summary of the development proceedings and details the processes followed to develop the proposed Reliability Standard. These processes included, among other things, comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballot achieved a quorum, and the additional ballot and final ballot exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standard. No comments were received that indicated the proposed Reliability Standard conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.