UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL 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 7, 2019

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
FOR APPROVAL OF
PROPOSED RELIABILITY STANDARD CIP-008-6

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] the North American Electric Reliability Corporation ("NERC")[3] hereby submits for Commission approval proposed Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning. The proposed Reliability Standard addresses the Commission's directive from Order No. 848[4] to develop modifications to require reporting of Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's[5] 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 Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT").[6] In

---

1 16 U.S.C. § 824o (2018).

2 18 C.F.R. § 39.5 (2018).

3 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

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

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

6 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").

addition, the proposed modifications require specific information in Cyber Security Incident reports and include deadlines for submitting the reports as directed by the Commission.

NERC requests that the Commission approve the proposed Reliability Standard, provided in Exhibit A hereto, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also requests approval of:

- 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 Commission-approved Reliability Standard CIP-008-5.

As required by Section 39.5(a) of the Commission's regulations,[7] this Petition 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 criteria identified by the Commission in Order No. 672[8] (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,[9] minimize loss and destruction, mitigate weaknesses that were exploited, and help to restore capabilities. The

---

7 18 C.F.R. § 39.5(a).

8 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 ("Order No. 672"), *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

9 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.

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 modifications address the Commission'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.[10] Consistent with the Commission'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.[11]

Proposed Reliability Standard CIP-008-6 addresses the Commission'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

[10] Order No. 848 at P 2.

[11] *Id*. at PP 2-3.

- 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 successor to ICS-CERT[12]: (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.

[12] 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.

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.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[13]

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) an explanation of the regulatory framework for NERC; (b) a description of the NERC Reliability Standards

[13] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

Development Procedure; (c) an overview of the Order No. 848 directive addressed in this Petition; and (d) the history of the Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting.

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[14] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[15] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[16] Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[17]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the

---

14 16 U.S.C. § 824o.

15 *Id*. § 824o(b)(1).

16 *Id*. § 824o(d)(5).

17 18 C.F.R. § 39.5(a).

Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[18]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[19] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[20] In its ERO Certification Order, the Commission found that NERC's proposed 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 Standards.[21] 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 Commission for approval.

C. Order No. 848

Order No. 848 adopts the proposals included in a Notice of Proposed Rulemaking issued on December 21, 2017.[22] In Order No. 848, the Commission directed NERC to develop and submit

---

18 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

19 Order No. 672 at P 334.

20 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.

21 ERO Certification Order at P 250.

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

modifications to the NERC Reliability Standards to augment mandatory reporting of Cyber Security Incidents.[23] The Commission directed the modifications to be submitted to FERC within six months of the effective date of Order No. 848.[24] Specifically, the Commission 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.

The Commission also directed NERC to submit an annual anonymized, public summary of the reports to the Commission.[25]

As mentioned above, the Commission 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."[26] The Commission also directed NERC to develop reporting timelines that consider the severity of the event and the risk to BES reliability.[27]

---

23 Order No. 848 at P 16.

24 *Id*. at P 37.

25 Order No. 848 at P 16.

26 *Id*. at P 91.

27 *Id*. at P 89.

The Commission also provided guidance on certain aspects of how NERC should identify EACMS for reporting purposes and define "attempts to compromise." With regard to EACMS, the Commission 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.[28] With regard to the definition of "attempted compromise" for reporting purposes, the Commission stated it "considers attempted compromise to include an unauthorized access attempt or other confirmed suspicious activity."[29]

D. 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 the Commission'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 during the last 5 days of the comment period.[30] 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.[31] The second draft of proposed Reliability Standard CIP-008-6 received the requisite approval with affirmative votes of

---

28 *Id*. at P 54.

29 *Id*. at P 55.

30 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.

31 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.

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.[32] The Board adopted the proposed Reliability Standard on February 7, 2019.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standard addresses the Commission'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).

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;

[32] 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.

- 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, the Commission 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 the Commission. 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 the Commission'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 the Commission'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."[33]

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 the Commission in Order

[33] *See* Exhibit A to this Petition, 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.

No. 848 (i.e., authentication, monitoring and logging, access control, Interactive Remote Access, and alerting).[34]

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[35] ("EAP") on the ESP can be considered an EACMS. Any attempts on the EAP would be brought into scope based on 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;[36]
- Adding processes to identify Cyber Security Incidents that are attempts to compromise applicable systems; and

---

34 Order No. 848 at P 54.

35 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.

36 Applicable systems refers to high and medium impact BES Cyber Systems and their associated EACMS.

- 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.~~[37]

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.

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

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.[38]

As noted in previous Petitions 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.[39] 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.[40]

---

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

[39] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-003-7*, at 22-24, Docket No. RM17-11-000 (Mar. 3, 2017).

[40] 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

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.

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**.[41]

Similar to the revisions in Requirement R1, the revisions to Requirement R2 address the component of the Commission'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.

---

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.

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

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),[42] 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*.

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.

[42] 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).

Proposed Requirement R4 addresses the Commission'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, the Commission 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.[43]

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.

[43] Order No. 848 at P 90.

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 the Commission 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."[44] 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 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."[45] While recognizing the need for prompt reporting of such incidents, the standard

44 *Id*. at P 89.
45 *Id*.

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 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 FERC-approved changes to the NERC Compliance Registry under the risk-based registration initiative.[46]

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.[47]

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.[48]

---

[46] *Order on Electric Reliability Organization Risk Based Registration Initiative and Requiring Compliance Filing*, 150 FERC ¶ 61,213 (2015) (approving removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

[47] In Order No. 818, the Commission approved NERC's revised definition of the term "Remedial Action Scheme" and approved certain Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes". *Revisions to Emergency Operations Reliability Standards; Revisions to Undervoltage Load Shedding Reliability Standards; Revisions to the Definition of "Remedial Action Scheme" and Related Reliability Standards*, Order No. 818, 153 FERC ¶ 61, 228 (2015).

[48] 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.

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.[49] 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 Commission 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.

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standard to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan provides that the proposed Reliability Standard and the modified NERC Glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the Commission's order approving the proposed Reliability Standard. As to the proposed modified definitions, the Implementation Plan provides that their effective date corresponds to the effective date of proposed Reliability Standard CIP-008-6.

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

[49] Order No. 672 at P 327.

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 the order 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.[50]

[50] The Commission considers how the implementation plan, "balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability." Order No. 672 at P 333.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve:

- proposed Reliability Standard CIP-008-6, and associated elements included in Exhibit A and G;
- the proposed Implementation Plan included in Exhibit B;
- the revised definitions to be incorporated into the NERC Glossary included in Exhibit A; and
- the retirement of Commission-approved Reliability Standard CIP-008-5.

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 7, 2019

Exhibit A

Proposed Reliability Standards

Exhibit A

Reliability Standard CIP-008-6 Clean and Redline

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 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 Reportable Cyber Security Incident; 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.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

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].*

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.*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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),[1] 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:
None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)	the "Applicable Systems" column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response to a Reportable Cyber Security Incident. (3.1.3)	Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days	Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity	Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a		The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-~~5~~6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in theirits documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it ~~makes sense and~~ is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact

and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002~~-5~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002~~-5~~ identification and categorization processes.

B. Requirements and Measures

~~R2.~~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-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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~~; or • An attempt to compromise, as determined by applying the ~~Electricity Sector Information Sharing~~criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and ~~Analysis Center (ES-ISAC), unless prohibited by law. Initial~~ 1.2.3 To provide 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~~	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents ~~and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).~~ or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		~~Incident.~~per Requirement R4.	
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and -Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and -Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents- and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

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-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

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-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

CIP-008-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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),[1] 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:
None

2. ~~2.~~ Table of Compliance Elements

~~—~~R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**~~-~~Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents~~.~~ or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)	system identified in the "Applicable Systems" column for Part 1.2. (1.2) ~~OR~~ ~~The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)~~
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan~~.~~(s). (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months between tests of the plan~~.~~(s). (2.1)	months between tests of the plan~~.~~(s). (2.1)	months between tests of the plan~~.~~(s). (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident ~~occurs. (2.2)~~or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents~~.~~ ~~(2.3)~~ or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less	Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that	Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing

this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. 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, multi-discipline 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*. 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.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

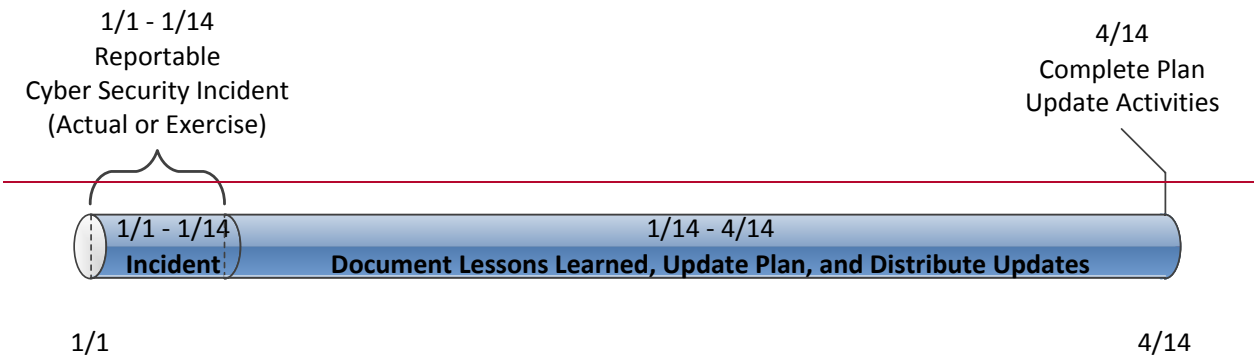


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. 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.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

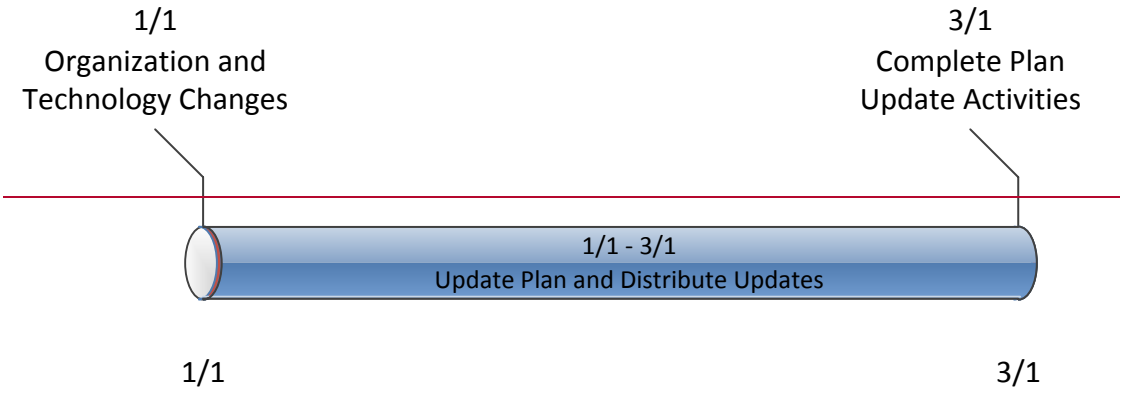


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures

~~the plan represents the actual response and does not exist for documentation only. 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.~~

~~**Summary of Changes:** Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.~~

~~**Reference to prior version:** (Part 2.1) CIP-008, R1.6~~

~~**Change Description and Justification:** (Part 2.1)~~

~~*Minor wording changes; essentially unchanged.*~~

~~**Reference to prior version:** (Part 2.2) CIP-008, R1.6~~

~~**Change Description and Justification:** (Part 2.2)~~

~~*Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*~~

~~**Reference to prior version:** (Part 2.3) CIP-008, R2~~

~~**Change Description and Justification:** (Part 2.3)~~
~~*Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*~~

~~**Rationale for R3:**~~

~~Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.~~

~~**Summary of Changes:** Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.~~

~~**Reference to prior version:** (Part 3.1) CIP-008, R1.5~~

~~**Change Description and Justification:** (Part 3.1)~~

~~*Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*~~

~~**Reference to prior version:** (Part 3.2) CIP-008, R1.4~~

~~**Change Description and Justification:** (Part 3.2)~~

~~*Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/6/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Definition of Terms Used in Standards

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms

Cyber Security Incident:
A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that 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.

Redlined to Last Approved

Proposed Modified Terms

Cyber Security Incident:

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, ~~C~~compromises~~,~~ or ~~was an~~ attempts 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~~ attempts to disrupt~~,~~ the operation of a BES Cyber System.

Reportable Cyber Security Incident:

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.

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard and Definitions

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident

Requested Retirements

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident (currently effective definition)
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident (currently effective definition)

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of this project is to address the directives that FERC issued in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the Reliable Operation of the Bulk

Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the four elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center (NCCIC)[1].

Effective Date

Reliability Standard CIP-008-6
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.

Revised Definitions for Cyber Security Incident and Reportable Cyber Security Incident
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.

[1] 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).

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.

Retirement Date

Reliability Standard CIP-008-5
Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Currently Effective Definitions for Cyber Security Incident and Reportable Cyber Security Incident
The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standard meets or exceeds the 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.[2]**

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 Commission directive in Order No. 848.[3] 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

---

1 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

2 Order No. 672 at PP 321, 324.

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

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 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.[4]

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. 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.[5]

The Violation Risk Factors and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and Commission 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

---

4 Order No. 672 at PP 322, 325.

5 Order No. 672 at P 326.

violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

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.** [6]

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.**[7]

The proposed Reliability Standard achieves the reliability goals effectively and efficiently in accordance with Order No. 672. 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.**[8]

---

6 Order No. 672 at P 327.

7 Order No. 672 at P 328.

8 Order No. 672 at P 329-30.

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. The proposed Reliability Standard satisfies the Commission'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.**[9]

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.**[10]

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.**[11]

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

---

9 Order No. 672 at P 331.

10 Order No. 672 at P 332.

11 Order No. 672 at P 333.

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 Commission-approved Reliability Standard development process.[12]

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved, 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.[13]

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.[14]

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

---

12 Order No. 672 at P 334.

13 Order No. 672 at P 335.

14 Order No. 672 at P 323.

Exhibit D

Consideration of Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Augment reporting to include Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems	FERC Order No. 848, P 3	The Project 2018-02 Standard Drafting Team (SDT) agrees that Reliability Standards include mandatory reporting of Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter (ESP) or associated Electronic Assess Control or Monitoring Systems (EACMS) and therefore proposes modification of NERC Glossary of Terms definitions for Cyber Security Incident and Reportable Cyber Security Incident and proposes the addition of EACMS associated with High and Medium BES Cyber Systems as applicable systems for requirements CIP-008 R1, R2, R3, and R4.
Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Specifically, the minimum set of attributes to be reported should include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or	FERC Order No. 848, P 3 and P 13	The SDT agrees that Cyber Security Incident reports should include certain minimum information detailed in FERC Order No. 848 P 3 and P 13 to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. The SDT drafted CIP-008 R4 to address the minimum set of attributes to include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or attempt to achieve the Cyber Security

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
attempt to achieve the Cyber Security Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident.		Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident.
Filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a Responsible Entity	FERC Order No. 848, P 3	The SDT agrees that the filing deadlines for Cyber Security Incident Reports should be established as identified in FERC Order No. 848, paragraph 3. The SDT proposes the addition of CIP-008 Requirement R4 to establish report filing deadlines for a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, once it is identified by a Responsible Entity pursuant to documented processes required in Requirement R1.
Reports should continue to be sent to the E-ISAC, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	FERC Order No. 848, P 3	The SDT agrees that reports should be submitted to the E-ISAC and the United States National Cybersecurity and Communications Integration Center (NCCIC), which is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and proposes the addition of CIP-008 Requirement R4 to establish reporting obligations. Requirement R4 includes the requirement to notify E-ISAC and NCICC once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, has been identified by the Responsible Entity pursuant to the processes under Requirement R1. The SDT did not modify any language that would remove or alter the obligation to report to DHS through EOP-004 or OE-417.

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
With regard to identifying EACMS for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting. Reporting a malicious act or suspicious event that has compromised, or attempted to compromise, a responsible entity's EACMS that perform any of these five functions would meet the intended scope of the directive by improving awareness of existing and future cyber security threats and potential vulnerabilities. In a similar vein, the assets (i.e., EACMS) subject to the enhanced reporting requirements should be identified based on function, as opposed to a specific technology that could require a modification in the reporting requirements should the underlying technology change.	FERC Order No. 848, P 54 and P 70	The SDT agrees that for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. The proposed new definitions, Cyber Security Incident and Reportable Cyber Security Incident, identify Cyber Security Incidents that attempt to compromise or disrupt an EACMS of a high or medium impact BES Cyber System. The SDT asserts that the five functions included in FERC Order No. 848, paragraph 54 and 70, are the essence of an EACMS by the current definition and proposed its inclusion in the modified definitions.
With regard to timing, we conclude that NERC should establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT based on a risk impact assessment and incident prioritization approach to incident reporting. This approach would establish reporting timelines that	FERC Order No. 848, P 89	The SDT agrees that reporting timelines should be established for when the Responsible Entity must submit Cyber Security Incident reports to the E-ISAC and NCCIC based on a risk impact assessment, as identified in FERC Order No. 848, paragraph 89. The SDT proposes the addition of CIP-008 Requirement R4 to establish reporting timelines for when the responsible entity

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
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.		must submit Cyber Security Incident reports to the E-ISAC and NCCIC. The initial notification timelines are identified in the proposed Requirement R4, Part 4.2, and the update timelines are identified in the proposed Requirement R4, Part 4.3. The proposed reporting timelines 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.

(i)

Exhibit E

Implementation Guidance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 2019 - DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Incident Reporting and Response Planning

Implementation Guidance for CIP-008-6

RELIABILITY | ACCOUNTABILITY




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

Table of Contents

List of Figures

Introduction

The Standards Project 2018-02 – Modifications to CIP-008 Standard Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-008-6. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1]

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP- 008-6.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 848 on July 19, 2018, calling for modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.[2] The Commission directed the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the Reliability Standards 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).[3]

The Commission's directive consisted of four elements intended to augment the current Cyber Security Incident reporting requirement: (1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) now known as NCCIC[4]. Further, NERC must file an annual, public, and anonymized summary of the reports with the Commission.

The minimum attributes to be reported should 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.

The Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require responsible entities to meet the directives set forth in the Commission's Order No. 848.

---

[1] NERC's Compliance Guidance Policy

[2] 16 U.S.C. 824o(d)(5). The NERC Glossary of Terms Used in NERC Reliability Standards (June 12, 2018) (NERC Glossary) defines a Cyber Security Incident as "A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."

[3] The NERC Glossary defines "ESP" as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." The NERC Glossary defines "EACMS" as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

[4] The DHS ICS-CERT underwent a reorganization and rebranding effort and is now known as the National Cybersecurity and Communications Integration Center (NCCIC).

Definitions

CIP-008-6 has two related definitions, as well as language for "attempts to compromise" that is specific to CIP-008-6 within Requirement R1 Part 1.2.2. Cyber Security Incidents are not reportable until the Responsible Entity determines one rises to the level of a Reportable Cyber Security Incident or meets the Responsible Entity's established criteria for attempts to compromise pursuant to Requirement R1 Part 1.2.1 and 1.2.2. When these thresholds are reached reporting to both E-ISAC and NCCIC (Formerly DHS's ICS-CERT) is required. These definitions and requirement language are cited below for reference when reading the implementation guidance that follows.

Cyber Security Incident:
A malicious act or suspicious event that:

- For high or medium Impact BES Cyber Systems, compromises, or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that 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.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications		
Part	**Applicable Systems**	**Requirements**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 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 Reportable Cyber Security Incident, 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.

The determination of reportability for compromises or disruptions (by definition), or for attempts to compromise (pursuant to the requirement language), becomes a function of applying criteria that builds upon the parent definition of Cyber Security Incident.

A color code that progresses from no reportability to greatest reportability is used in Figure 1.

GREEN	YELLOW	ORANGE	RED
non-reportable events/activity, or determination not made	is Cyber Security Incident, reportable determination not made	is determined reportable attempt to compromise an Applicable System	is determined Reportable Cyber Security Incident

The below Venn diagram illustrates the relationships between the elements of each definition, and the Requirement R1 Part 1.2.2 requirement language. In this example, one potential option could be to leverage the EACMS function descriptors noted in FERC Order 848 Paragraph 54 as criteria. This could serve as an approach to assess operational impact and/or functionality of cybersecurity controls that cause a Cyber Security Incident to rise to either level of reportability:

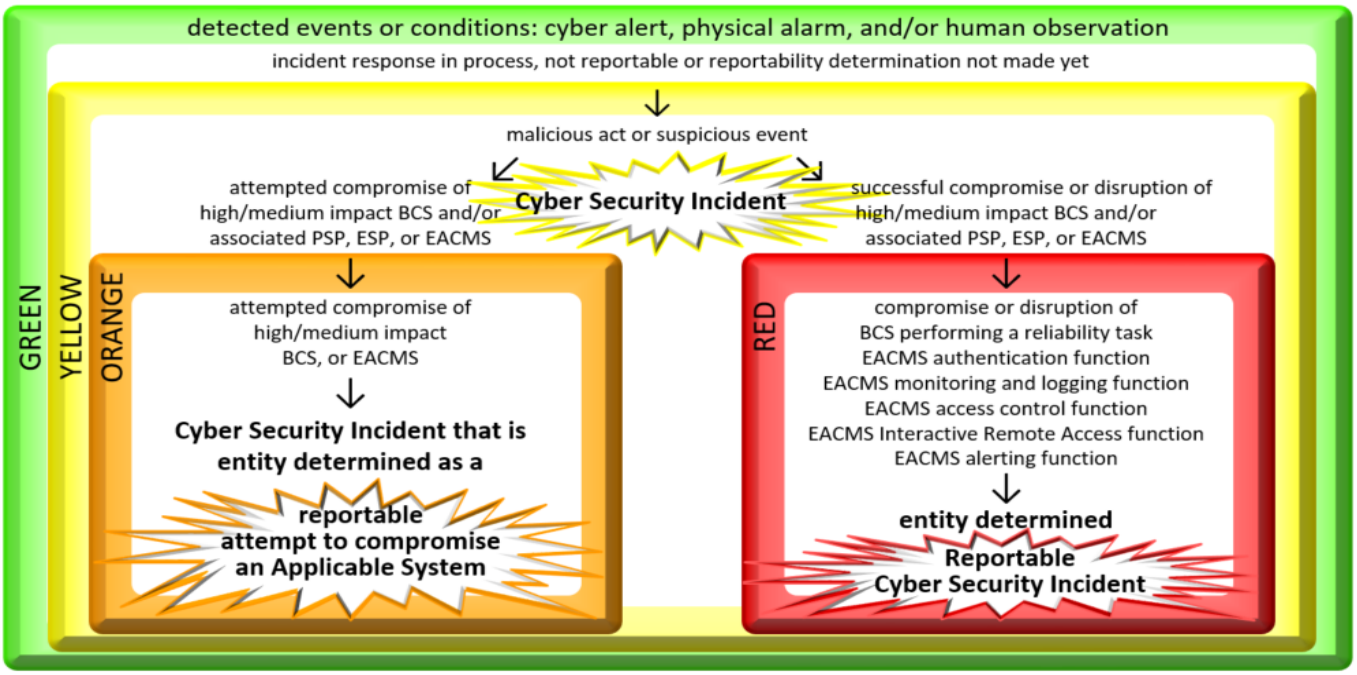


Figure 1 Relationship of Cyber Security Incidents

As shown in the above diagram, there is a progression from identification through assessment and response before a detected event or condition elevates to a reportable level.

First, the Registered Entity must determine the condition meets the criteria for a Cyber Security Incident.

Once the response and assessment has led to a Registered Entity's determination that events or conditions meet the definition of Cyber Security Incident, additional evaluation occurs to determine if established criteria or thresholds have been met for the Registered Entity to determine the Cyber Security Incident qualifies for one of the two reportable conditions:

1. Reportable Cyber Security Incident.
2. An attempt to compromise one or more systems identified in the "Applicable Systems" column for Requirement R4 Part 4.2 (pursuant to Responsible Entity processes and established attempt criteria documented in accordance with Requirement R1 Part 1.2)

Once the response and investigation has led to a Registered Entity's determination that the Cyber Security Incident has targeted or impacted the BCS performing reliability tasks and/or cybersecurity functions of the Applicable Systems, associated Cyber Assets, and/or perimeters, the notification and reporting timeframes and obligations begin. Note: Initial (or preliminary) notification is needed within the specified timeframe after this determination, even if required attributes (functional impact, level or intrusion, attack vector) are not yet known.

Once this initial notification is made, if all attributes were known, they should have been included in the initial notification and the reporting obligation ends.

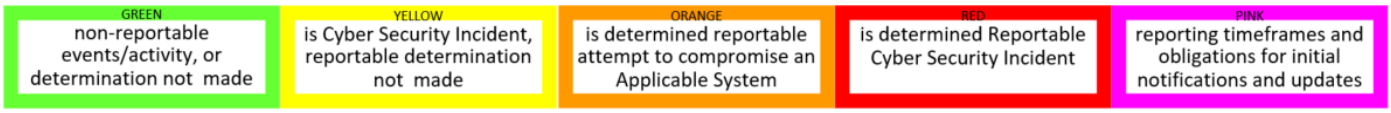
If all attributes were not known by the time the initial notification had to be made, the update timeframes trigger from the time the next attribute(s) is determined to be learned/known.

A Registered Entity's reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC, either during the initial notification or subsequently through one or more updates made commensurate with the reporting timeframes.

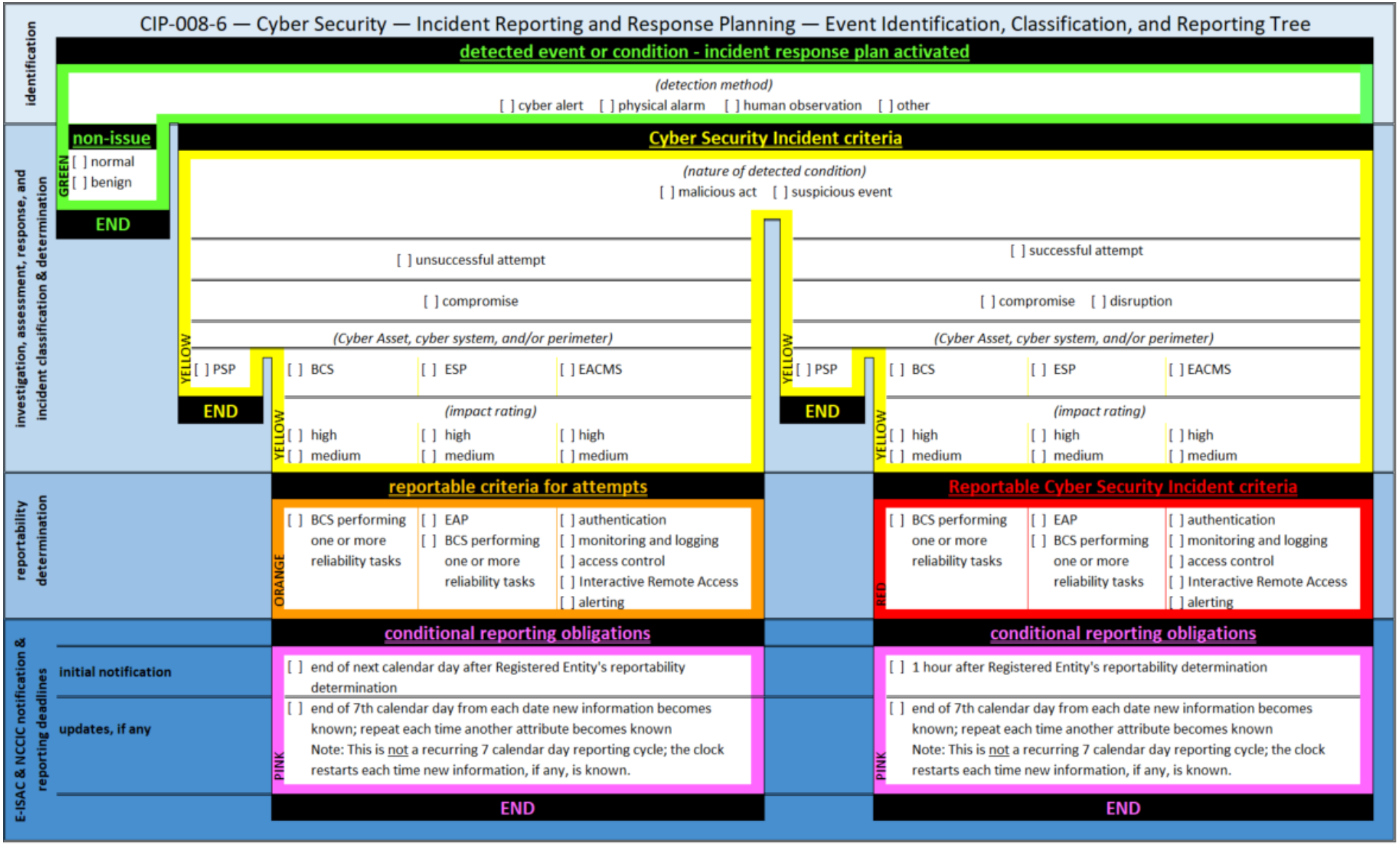
Determination and Classification of Cyber Security Incidents

Registered Entities may want to consider developing tools illustrating established process criteria that must be met, by definition, as well as the impacted/targeted operational task/cybersecurity functions considered to reach each incident classification and reporting threshold. The below decision tree is one potential approach Registered Entities could employ as a tool to assess events and make the Registered Entity determinations according to process(es) and established criteria documented pursuant to Requirement R1 Parts 1.1 and 1.2. Note: Where the term "criteria" is used in the optional tool examples, it is intended to serve as a section the entity may tailor to match the criteria they have included in their process(es). What is included in this guidance is not prescriptive and only one potential approach.

A similar color code to the diagram depicting the relationships between definitions and requirement language has been used to illustrate a progression from no reportability to greatest reportability inclusive of the respective reporting obligations and timeframes for initial notifications and updates for Figure 2 and Figure 3.



The blue shading in Figure 2 simply represents the distinction between phases in the incident response process as analysis and investigative actions occur and information unfolds.



*Where 'calendar day' is used, the 'end' of the day = 11:59 PM local time of that day.

** Where 'determination' is used, this refers to the Registered Entity's determination.

Figure 2 Potential Approach Tool

A second potential approach could be a flow diagram illustrating an entity's criteria and determination process as depicted in the example below:

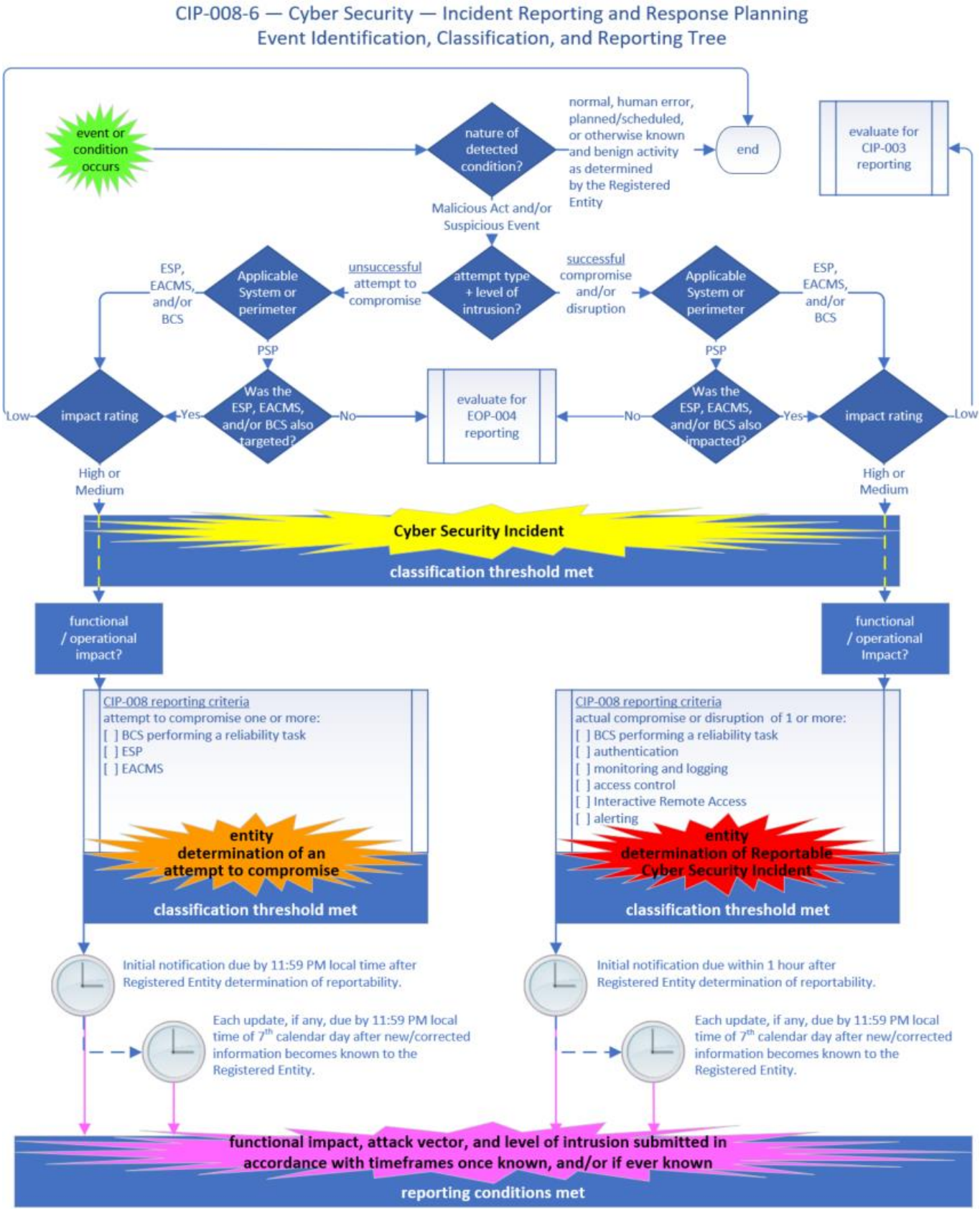


Figure 3: Flow Diagram for Cyber Security Incidents

Example of a Cyber Incident Classification Process

Entities may use a risk analysis-based method for the classification of cyber incidents and determination of Cyber Security Incidents, Reportable Cyber Security Incidents or, Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The risk analysis-based approach allows entities the flexibility to customize the appropriate response actions for their situation without being administratively burdened by a one size fits all solution. Entities also have the flexibility to incorporate their existing incident management processes which may already define how they classify and determine cyber incidents.

A risk-based approach considers the number of cyber security related event occurrences, the probability that the events will have an impact on their facilities, and severity of the impact of the event. This allows the entity to decide when cyber events should be investigated as cyber incidents, the classification of cyber incidents and the determination of when a cyber incident should be reported; either as part of a voluntary action, as part of a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

Entities should also consider that appropriate reporting of cyber incidents helps other entities in similar situations. The reporting of the details of an incident serves to alert other entities so they may increase their vigilance and take timely preventive or mitigating actions. All entities stand to benefit from such shared information in the long run.

As an example, a typical infrastructure installation is depicted in Figure below.

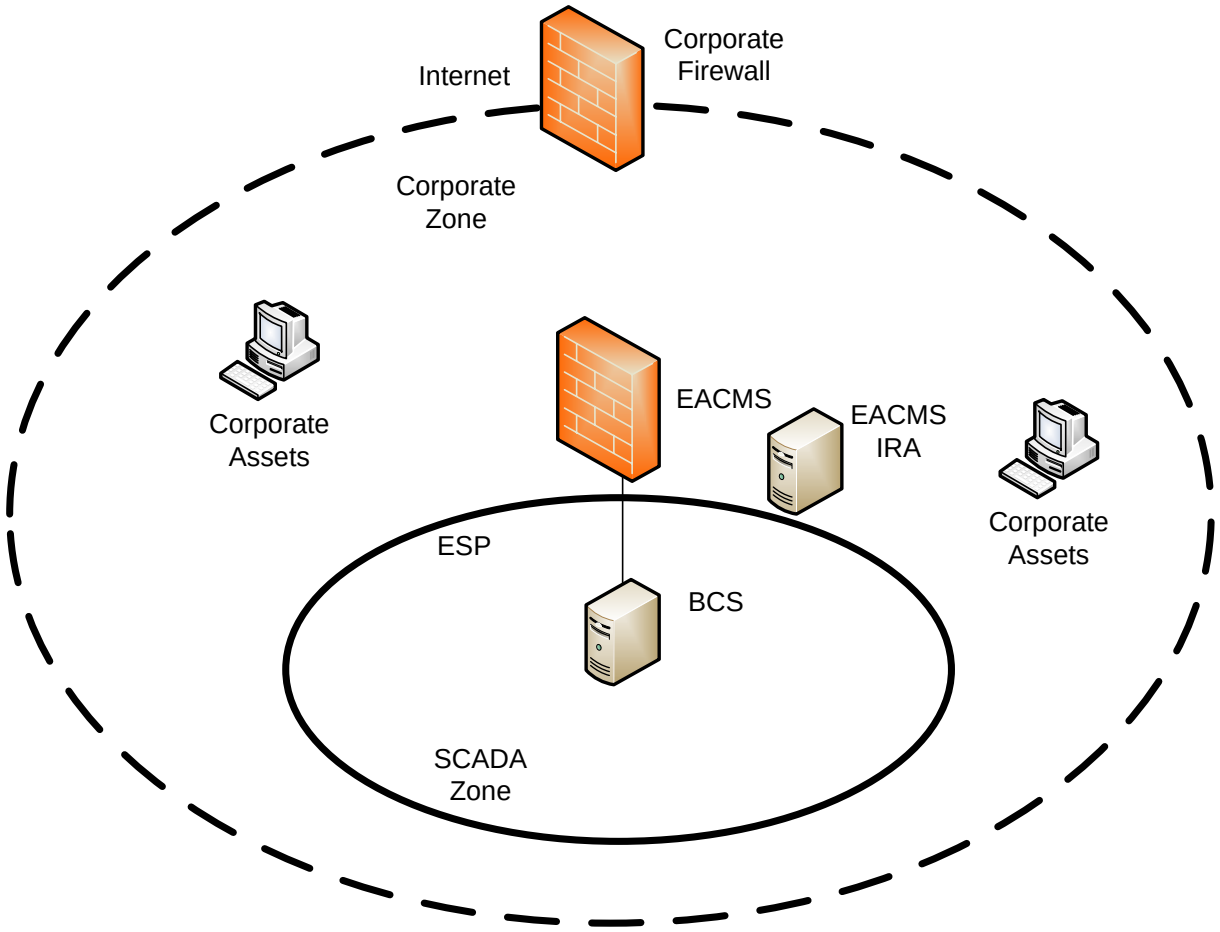


Figure 4 Typical Infrastructure

- A SCADA security zone consists of BES Cyber System (BCS), behind an Electronic Security Perimeter (ESP). The Electronic Access Point (EAP) is an interface of the SCADA firewall which is an Electronic Access Control or Monitoring System (EACMS).
- A Corporate security zone consists of regular corporate assets and other EACMS such as Intermediate Systems with Interactive Remote Access (IRA). A corporate firewall protects the corporate assets against intrusions from the Internet. The SCADA security zone is nested inside the corporate security zone.

Sample Classification Schema

A risk analysis could produce the incident categories below:

- Regular cyber events that represent a normal level of events where no further investigation is required such as random port-scans.
- Low risk incidents may be cyber events that become cyber incidents because they are beyond the normal level of events and require some type of investigation. Cyber incidents that are blocked at a firewall and found not to be malicious or suspicious could fall into this category.
- Medium risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and required mitigation activities.

  Note that while these cyber incidents were malicious or suspicious, they might not meet the definition of a Cyber Security Incident because the entity investigated and determined that the target was not a BCS, ESP, PSP or EACMS.

  For example, a corporate asset infected with well-known corporate malware and, as a result, is scanning the network to find other corporate assets. Although this activity is also being seen at the SCADA firewall (EACMS), the entity investigated and determined that this activity was not a Cyber Security Incident.
- High risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and did meet the definition of Cyber Security Incidents. For example, malicious malware on a corporate asset that repeatedly attempts to log into a SCADA IRA Intermediate System but is unsuccessful. This would be a Cyber Security Incident and should also fall into the entity's definition of a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part with the target being an EACMS (SCADA IRA Intermediate System).
- Severe risk incidents may be those Cyber Security Incidents that involves successful compromise of an ESP or EACMS and hence meet the criteria for Reportable Cyber Security Incident. These may also escalate into Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as the BCS.
- Emergency risk incidents may be those Cyber Security Incidents that compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity. These incidents may represent an immediate threat to BES reliability and may require emergency actions such as external assistance.

These incident categories can be mapped into a standard incident classification and reporting schema like the NCCIC Cyber Incident Scoring System[5]. This is a common schema used by the United States Federal Cybersecurity Centers for describing the severity of cyber incidents and is available to industry to leverage.

Utilizing the NCCIC schema as a basis for identification and classification of Cyber Security Incidents could be adapted to produce the schema below for application to CIP-008-6:

	General Definition	Consequences
Level 5 Emergency Black	A cyber incident that investigation found was a Cyber Security Incident that has compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity.	Incidents that result in imminent threat to public safety and BES reliability. A Reportable Cyber Security Incident involving a compromise or disruption of a BCS that performs one or more reliability tasks of a functional entity.
Level 4 Severe Red	A cyber incident that investigation found was a Cyber Security Incident involving a compromise or disruption of an ESP or EACMS; OR A cyber incident that investigation found was a Cyber Security Incident that attempted to compromise a BCS.	Cyber Security Incidents that have the potential to result in a threat to public safety and BES reliability if malicious or suspicious activity continues or escalates. Immediate mitigation is required. A Reportable Cyber Security Incident involving a compromise or disruption of a EACMS or ESP OR A Cyber Security Incident that must be reported as an attempt to compromise or disrupt a BCS
Level 3 High Orange	A cyber incident that investigation found met the entity's defined criteria for a Cyber Security Incident that attempted to compromise or disrupt an EACMS or ESP	An attempt to compromise an EACMS does not result in a threat to public safety or BES reliability, but still requires mitigation. A Cyber Security Incident that must be reported as an attempt to compromise or disrupt an EACMS
Level 2 Medium Yellow	A cyber incident that investigation found was malicious or suspicious but was not a Cyber Security Incident because it did not target an Applicable System or perimeter.	A cyber incident that does not represent a threat to public safety or BES reliability, even though it is malicious or suspicious and required mitigation.
Level 1 Low Green	A cyber incident that investigation found was not malicious or suspicious.	A cyber incident that does not represent a threat to public safety.
Level 0 Baseline White	Inconsequential cyber events.	Cyber events that require no investigation and are not cyber incidents. These do not represent a threat to public safety.

Figure 5 Example of Classification Schema

Reliability tasks may be those tasks that a Responsible Entity determines are associated with the BES Reliability Operating Services (BROS) listed in the NERC Functional Model.

[5] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Examples of the use of the Sample Classification Schema

Some examples of the use of the classification schema are listed below. The event number corresponds to the events depicted in the subsequent figures. The color code defined in the sample schema in Figure 5 is carried through Figures 6- 8.

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
External firewall scan (N1 – no color)	External IPS log Review of F/W log	External IPS Corporate F/W rules	No	No	No	Determined by entity as regular background activity
Corporate Zone internal scan by non-malicious source (existing network monitoring Tool) (N2 - no color)	Corporate IPS Review of EACMS – IRA host F/W Log (CIP-007 R4)	Corporate IPS EACMS IRA Host F/W	No	No	No	Determined by entity as regular background activity – previously investigated and determined to be known source

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone internal scan by unknown source (N3 - green)	Corporate IPS Review of EACMS IRA host F/W Log	Corporate IPS IRA EACMS Host F/W	Yes	No	No	Investigation found new network monitoring tool. Added to regular background activity.
Corporate Zone Internal scan by unknown source (N4 - yellow)	Corporate IPS Corporate Antivirus Review of EACMS IRA host F/W Log Review of EACMS SCADA F/W Log	Corporate IPS IRA EACMS Host F/W Corporate Anti-virus SCADA F/W EACMS	Yes	No	No	Investigation by entity determined malware in Corporate zone was targeting other corporate assets and not specifically the Applicable Systems. (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by EACMS IRA login attempts (N5 - orange)	Corporate IPS Review of EACMS IRA host F/W Log Review of EACMS IRA failed Logins (CIP-007 R4)	Corporate IPS EACMS host F/W EACMS login 2 factor	Yes	Yes EACMS – IRA targeted	Yes Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Investigation found malware in Corporate zone was an attempt to compromise one or more Applicable Systems - IRA Intermediate System - EACMS (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by successful EACMS IRA login and attempted BCS logins (N6 - red)	SCADA IPS log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS failed Logins (CIP-007 R4)	SCADA IPS (CIP-005 R1.5) BCS user/ password login	Yes	Yes	Yes EACMS – IRA host compromised or disrupted Reportable Cyber Security Incident BCS host failed logins Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as BCS	Investigation found malware compromised or disrupted EACMS IRA. Attempt to compromise a BCS. (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
BCS – SCADA system failure following Corporate Zone Internal scan by unknown source, successful EACMS IRA login and successful BCS login (N7 - black)	SCADA system log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS Logins (CIP-007 R4)	None	Yes	Yes	Yes Comprise or disruption of a BCS performing one or more reliability tasks of a functional entity Reportable Cyber Security Incident	Investigation found malware compromised a BCS performing one or reliability tasks of a functional entity

Figure 6 Examples of the Use of the Classification Schema

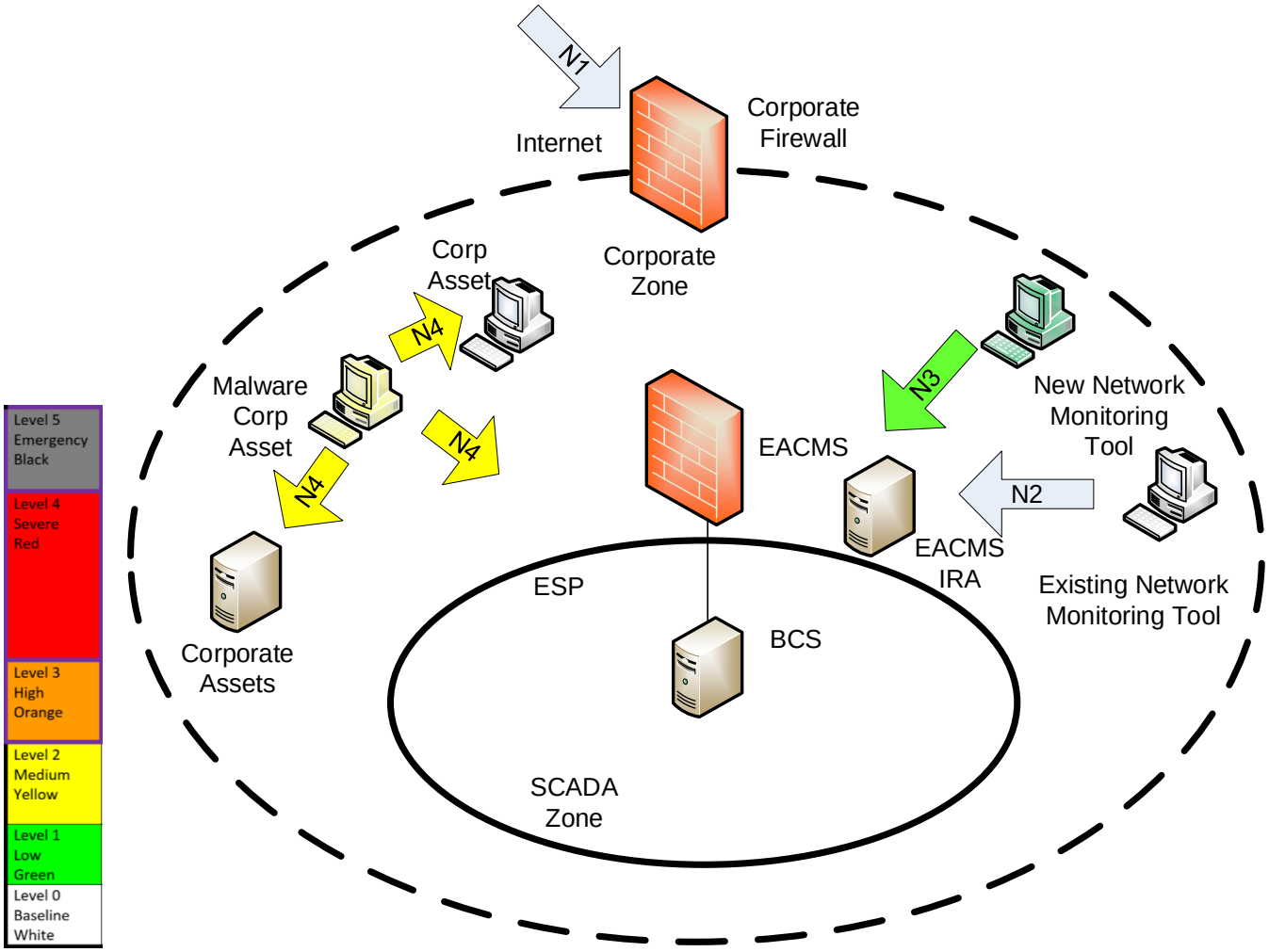


Figure 7 Examples of Non-Reportable Cyber Incidents

The figure above depicts examples of non-reportable cyber incidents using the sample classification schema and examples in Figure 6.

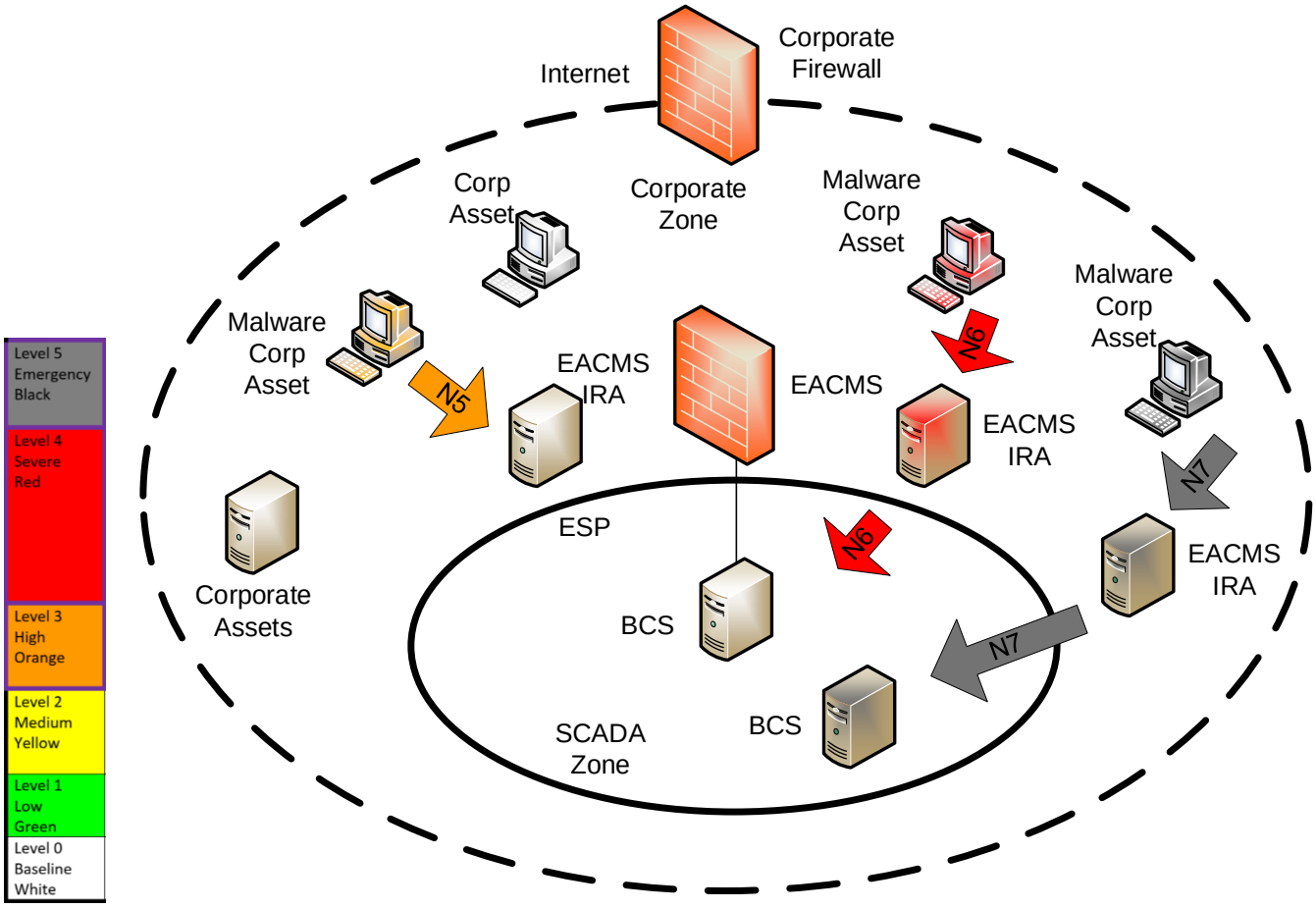


Figure 8 Examples of Reportable Cyber Security Incidents or attempt to compromise one or more applicable systems

The figure above depicts examples of Reportable Cyber Security Incidents or attempts to compromise one or more systems identified in the "Applicable Systems" column for the Part using the sample classification schema and examples in Figure 6.

Attempts to Compromise and Cyber Security Incidents

Registered Entities should evaluate and determine what is normal within their environment to help scope and define what constitutes 'an attempt to compromise' in the context of CIP-008, and should document established criteria within the entity processes. This can help Subject Matter Experts (SMEs) identify deviations from normal, and assist a Registered Entity in timely and effective incident determination, response, and vital information sharing.

Entities are encouraged to explore solutions designed to take the guess work out of the process without being overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs. Entities may want to consider options like a decision tree or a checklist for SMEs to apply defined criteria used to determine reportability.

As an example, an entity could define an "attempt to compromise" as an act with malicious intent to gain access or to cause harm to normal operation of a Cyber Asset in the "Applicable Systems" column. Using this sample definition, some criteria could be:

1. Actions that are **not** an attempt to compromise an applicable Cyber Asset/System electronically are:
   a. An entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence that is performed expected on demand or on an approved periodic schedule.
   b. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic, but it does not have malicious intent.
   c. Attempts to access a Cyber Asset by an authorized user that have been determined to fail due to human error.
2. Actions that **are** an attempt to compromise an applicable Cyber Asset/System electronically are:
   a. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management nor process(es). This could be from an entity's own equipment due to an upstream compromise or malware.
   b. Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.
   c. Attempts to escalate privileges on a Cyber Asset by an authorized user that has been determined to fail due to not being authorized for that privilege level.

Registered Entities may also want to evaluate system architecture for ways to limit exposure for 'attempts to compromise'. Techniques like the implementation of security zones and/or network segmentation can minimize the level of traffic that can get to applicable Cyber Assets and help minimize the attack surface.

Registered Entities with implementations that involve an EACMS containing both an Electronic Access Point (EAP) and a public internet facing interface are strongly encouraged to change this configuration in favor of architectures that offer layers of safeguards and a defense in depth approach.

Similarly, Registered Entities with implementations involving an EACMS containing both an EAP and a corporate facing interface to their business networks may also want to consider options to re-architect to reduce cyber events from the corporate environment such as broadcast traffic from causing extra administrative workload.

A color code that progresses from no reportability to greatest reportability is used in Figure 9.

Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

The table below contains examples of various degrees of events or conditions at varied levels of determination:

Event	Normal or Benign		Malicious / Confirmed Suspicious	
PSP breach	• Unauthorized user compromises the PSP to steal copper and the Registered Entity determines cybersecurity controls were not targeted and remain in place.	GREEN	• Unauthorized user breaks into a Substation control house (**CIP-006-6 R1.5 activates BES Cyber Security Incident response plan within 15 minutes of detection.**)	GREEN
			• Unauthorized user breaks into a Substation control house and inserts unauthorized Removable Media into an EACMS or BCS and the Registered Entity determines no interaction between the USB and the EACMS or BCS occurred. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
	• An equipment operator loses control of a backhoe and crashes into a control house, breaching the PSP and the Registered Entity determines it was accidental; cybersecurity controls were not targeted and remain in place.	GREEN	• Registered Entity determines the unauthorized Removable Media contains malware (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• Registered Entity determines the malware has harvested the credentials of a BCS, gained unauthorized access and disrupted a reliability task. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED
Port Scanning	• Registered Entity owned monitoring tool that runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at the expected time.	GREEN	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at an unexpected time and the Registered Entity has determined this as suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
	• A Registered Entity performs a port scan of an EACMS or BCS during a scheduled Cyber Vulnerability Assessment activity.	GREEN	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it is targeting specific ports relevant to the BCS. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it gained unauthorized access to the EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED

Event	Normal or Benign		Malicious / Confirmed Suspicious	
Detected malware	• A corporate machine infected by a known Windows-specific vulnerability is scanning all local hosts including non-Windows-based EACMS or BCS and is determined by the Registered Entity to be an SMB exploit applicable to only Windows-based machines.	GREEN	• An infected corporate machine is scanning all local hosts including an EACMS or BCS for well-known ports and determined to be a suspicious event by the Registered Entity. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and has attempted to gain unauthorized access to the EACMS or BCS. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and exploited/compromised specified ICS ports that perform command and control functions of a BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED
Login activity	• Authorized user exceeded the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login attempts against an EACMS or BCS and the Registered Entity confirmed the user incorrectly entered his/her password after performing annual password changes.	GREEN	• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity investigates that activity as a Cyber Security Incident because it is deemed suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**).	YELLOW
	• A system exceeds the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login against an EACMS or BCS and locks out a system account and the Registered Entity confirmed the system account's password had changed but the accessing application/service had not yet been updated to use the new password.	GREEN	• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and failed login attempts. (**Determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**).	ORANGE
			• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and successfully gains unauthorized access to an EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**).	RED

Figure 9 Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

Example of Sample Criteria to Evaluate and Define Attempts to Compromise

An entity may establish criteria to evaluate and define attempts to compromise based on their existing capabilities and facilities associated with the other CIP Standards.

The sample criteria listed below are examples and are not intended to be exhaustive.

CIP-005 R1.5:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Detected known malicious or suspected malicious communications for both inbound and outbound communications.

CIP-005 R2.1:

Require multi-factor authentication for all Interactive Remote Access sessions.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Repeated attempts to authenticate using multi-factor authentication

CIP-007 R4.1:

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;
4.1.2. Detected failed access attempts and failed login attempts;
4.1.3. Detected malicious code.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Successful login attempts outside of normal business hours
- Successful login attempts from unexpected personnel such as those who are on vacation or medical leave
- Detected failed access attempts from unexpected network sources
- Detected failed login attempts to default accounts
- Detected failed login attempts from authorized personnel accounts exceeding X per day
- Detected failed login attempts from authorized personnel accounts where the account owner was not the source
- Detected malicious code on applicable systems

CIP-007 R5.7:

Where technically feasible, either:

- *Limit the number of unsuccessful authentication attempts; or*
- *Generate alerts after a threshold of unsuccessful authentication attempts.*

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Account locked due to limit of unsuccessful authentication attempts exceeded more than X times per day
- Threshold of unsuccessful authentication attempts exceeds more than X every Y minutes

CIP-010 R2.1:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Detected unauthorized changes to the baseline configuration

An entity may establish additional criteria to evaluate and define attempts to compromise based on their infrastructure configuration:

Sample criteria:
Where investigation by entity determines that the specific activity, while malicious or/and suspicious:

- Attempt to compromise was not intended to target the “Applicable Systems”

Other Considerations

Protected Cyber Assets

A Protected Cyber Asset (PCA) is defined as:

> *One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.*[6]

It should be noted that PCAs are not one of the Applicable Systems and as such cyber incidents solely involving PCAs are not Cyber Security Incidents and are not reportable. Entities are encouraged to voluntarily report cyber incidents involving PCAs.

PCAs do reside within the ESP and as a result, some cyber incidents may be initiated on PCAs and later escalate into Cyber Security Incidents involving a BCS, the ESP or an EACMS.

Some examples are as follows:

1. A PCA is compromised or there was an attempt to compromise a PCA locally via removable media.

   This is not a Cyber Security Incident and is not reportable.

2. A PCA is compromised or there was an attempt to compromise a PCA from a source external to the ESP using an existing firewall rule.

   The compromise or attempt to compromise the ESP must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident, a Reportable Cyber Security Incident or an attempt to compromise.

3. A PCA is compromised or there was an attempt to compromise a PCA via an EACMS that has been compromised.

   The compromise of the EACMS must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident or a Reportable Cyber Security Incident.

4. A PCA is compromised and is also subsequently used as a pivot point to compromise or attempt to compromise a BCS.

   The compromise or attempt to compromise of the BCS must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident, a Reportable Cyber Security Incident or an attempt to compromise.

[6] NERC Glossary of Terms https://www.nerc.com/files/glossary_of_terms.pdf

Requirement R1

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].*

1.1. One or more processes to identify, classify, and respond to Cyber Security Incidents.

1.2. One or more processes:

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 Reportable Cyber Security Incident 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. Provide notification per Requirement R4.

1.3. The roles and responsibilities of Cyber Security Incident response groups or individuals.

1.4. Incident handling procedures for Cyber Security Incidents.

Applicable Systems for the four collective Parts in Requirement R1 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R1

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

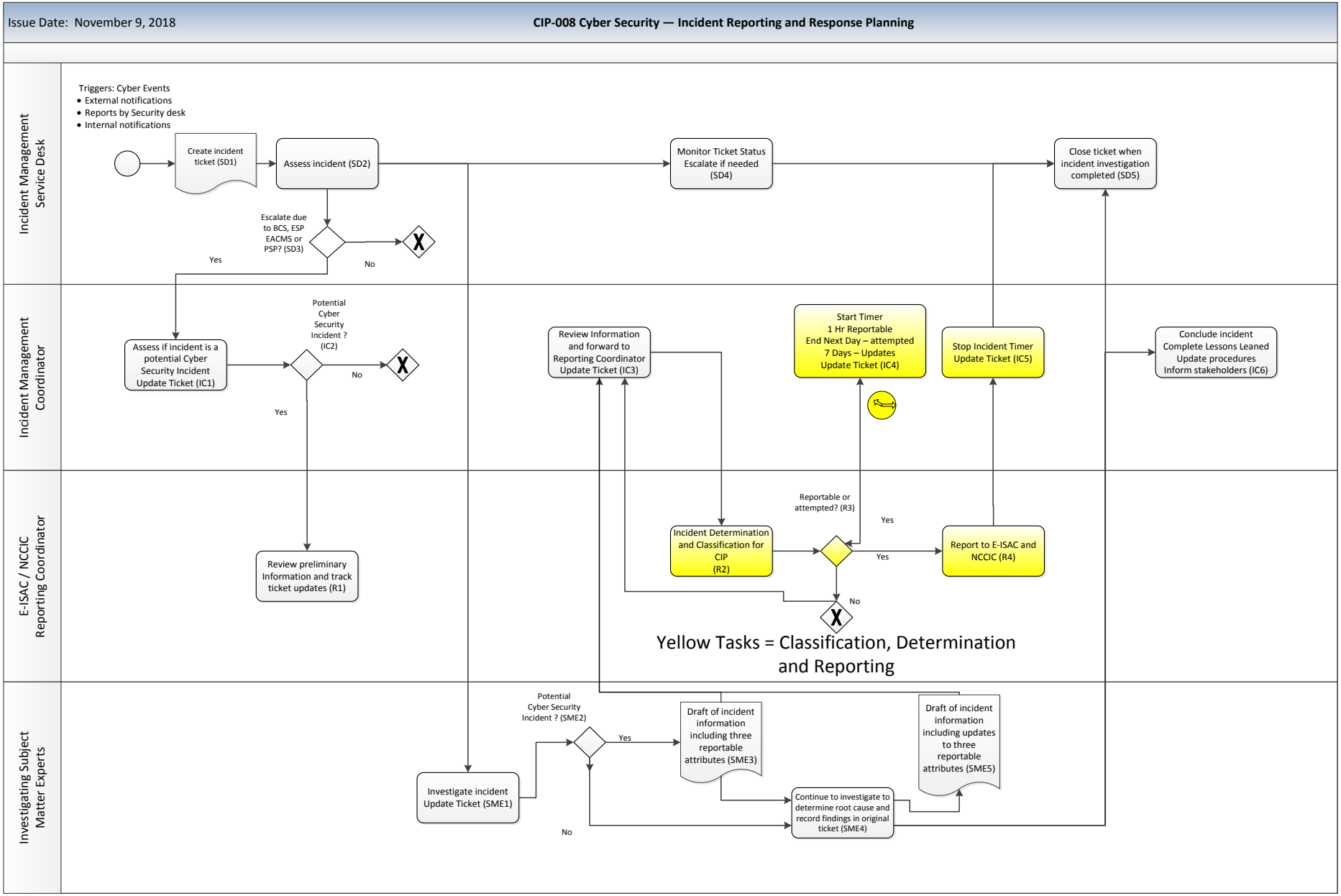


Figure 10 Sample Process to Identify, Classify and Respond to Cyber Security Incidents

Supporting Narrative Description of Sample Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

1. The Incident Management Service Desk identifies that a cyber event that requires investigation has occurred.
2. Incident Management Service Desk creates an incident ticket to log the suspected cyber incident (SD1).
3. Incident Management Service Desk performs initial assessment of the suspected cyber incident and performs any initial triage or service restoration as needed (SD2).
4. If the suspected cyber incident involves BES Cyber Systems (BCS), Electronic Access Control or Monitoring Systems (EACMS), Electronic Security Perimeter (ESP) or Physical Security Perimeters (PSP), the Incident Management Service Desk will escalate the incident to an Incident Management Coordinator whom will act as the coordinator until the incident is closed (SD3)
5. The Incident Management Coordinator performs a secondary initial assessment to determine if the incident has the potential to be a Cyber Security Incident, a Reportable Cyber Security Incident, or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

   They update the incident ticket, assigning the appropriate Investigating Subject Matter Experts (IC1).
6. If the Incident Management Coordinator determines that the incident has the potential to be reportable, the E-ISAC/ NCCIC Reporting Coordinator is alerted and copied on the information contained in the incident ticket. The E-ISAC/ NCCIC Reporting Coordinator continues to monitor the updates to the incident ticket (IC2).
7. The Incident Management Service Desk ensures the assigned Investigating SMEs are notified, and the incident ticket information is updated (SD2, SD4).
8. The assigned SMEs investigate the incident ticket updating with the Incident Management Coordinator as appropriate (SME1). The Incident Management Coordinator will monitor the progress of the investigation and assign additional SMEs or escalate as needed.
9. If initial investigation by SMEs finds that the incident may be a Cyber Security Incident and has the potential to be reportable (SME2), the SMEs will inform the Incident Management Coordinator and forward the known information including the required three attributes (SME3). Attributes which are unknown at the current time will be reported as "unknown".
10. The SMEs will continue their investigation to determine the root cause of the incident, performing triage or service restoration as needed, continue to investigate the three required attributes and update incident ticket information (SME4).
11. If the incident is found to be potentially reportable, the Incident Management Coordinator reviews the information, adds any details collected by other investigating SMEs and resolves any missing information as needed. The information is forwarded to the E-ISAC/ NCCIC Reporting Coordinator (IC3).
12. The E-ISAC/ NCCIC Reporting Coordinator reviews the information received, performs classification of the incident (R2). They determine if the incident is a Cyber Security Incident and determine if it is either a Reportable Cyber Security Incident or Cyber Security Incident that attempted to compromise

a system identified in the "Applicable Systems" column for the Part. The information to be reported is finalized (R3).

13. Upon determination that the incident is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a clock timer set to the appropriate time frame (IC4) and performs the required notification including the three required attributes. The incident ticket is updated with the incident classification and determination time for compliance evidence purposes:
    - Within 1 hour for initial notification of Reportable Cyber Security Incident,
    - By end of the next day for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, and
    - Within 7 calendar days of determination of new or changed attribute information required in Part 4.1, if any.

14. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator when notification is completed and time that the notifications occurred at. The Incident Management Coordinator will stop the appropriate timer and updates the incident ticket with the appropriate information for compliance evidence purposes (IC5).
15. If Incident Management Coordinator that has not received confirmation of notification, they may escalate, as needed, prior to expiry of the applicable timer. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4).
16. During the continued investigation of the incident (SME4), the SMEs may find that an update of any of the three required attributes is potentially required. The SMEs will inform the Incident Management Coordinator and forward a draft of the updated information (SME5)
17. The Incident Management Coordinator reviews the draft update information including adding other details, and then informs E-ISAC/ NCCIC Reporting Coordinator, forwarding the potential update information (IC3).
18. The E-ISAC/ NCCIC Reporting Coordinator reviews the potential updated information and determine if the update to any of the three required attributes is reportable (R3).
19. Upon determination that the update is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a timer set to the appropriate time frame (i.e. 7 calendar days). The incident ticket is updated with the determination time for compliance evidence purposes (IC4).
20. The E-ISAC/ NCCIC Reporting Coordinator updates both E-ISAC and NCCIC with the information associated with any of the three required attributes (R4).
21. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator that the update to E-ISAC and NCCIC is completed and times that the updates occurred at. The Incident Management Coordinator will stop the appropriate timer and update the incident ticket with the appropriate information for compliance purposes (IC5).

22. If the Incident Management Coordinator has not received confirmation that the update is completed, prior to the expiration of the timer, they may escalate as needed. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4).
23. Upon closure of the incident, the Incident Management Coordinator will ensure that the last reportable update to the three required attributes accurately reflects the closure information. If a further update of the three required attributes is required, the Incident Management Coordinator will inform the appropriate Subject Matter Expert to initiate an update (SME5).
24. The Incident Management Coordinator informs the Incident Management Service Desk that the incident ticket may be closed (SD5).
25. The Incident Management Coordinator will initiate a "Lessons Leaned" session and update to the Cyber Incident Reporting and Response Plan and any other documentation, procedures, etc. within 90 days (IC6). They will inform all stakeholders of any updates to the Cyber Incident Reporting and Response Plan and any other applicable documentation.

Roles and Responsibilities (R1.3)

In the example process, the defined Roles and Responsibilities are as follows, but can be tailored by any entity to align with their unique organization:

- Incident Management Service Desk is responsible for initial activities, incident ticketing and incident logging:
    - Initial identification, categorization and prioritization,
    - Initial diagnosis and triage/service restoration,
    - Initial assignment of incident tickets to Investigating Subject Matter Experts (SMEs)
    - Initial escalation to an Incident Management Coordinator upon assessment (if needed)
    - Monitoring incident ticket status and initiating further escalation (if needed)
    - Incident ticket resolution and closure
    - General incident status communication with the user community

- Incident Management Coordinator is responsible for the over-all coordination of activities related to an assigned incident:
    - Detailed assignment of tasks to Investigating SMEs
    - Ensure that all assigned activities are being performed in a timely manner
    - Ensuring regulatory reporting time limits are met and initiating escalation if needed
    - Communicating incident status with major affected stakeholders
    - Coordinating with the Incident Management Service Desk to update incident tickets with status and the logging of required details and assisting them to perform general incident status communications with the user community

- Coordinating with the E-ISAC/NCCIC Reporting Coordinator for cyber incidents with the potential of being Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Assisting the E-ISAC/NCCIC Reporting Coordinator with information to aid in the classification of the cyber incident.
- Escalation as needed according to the priority and severity of the issue
- Coordination of service restoration and incident closure
- Coordination of incident review following closure of incidents, identification of potential problems and documenting the "Lessons Learned"
- Initiating update of processes or procedures as needed and communicating the updates to stakeholders

- E-ISAC/ NCCIC Reporting Coordinator is responsible for the coordination of regulatory reporting activities such as those related to E-ISAC and NCCIC:
  - Review of completeness incident information for classification and reporting purposes
  - Incident classification for reporting purposes
  - Determination if this incident is a Cyber Security Incident, Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part
  - Completeness of the required three attributes to be reported
  - Notification to E-ISAC and NCCIC and submission of the three required attributes
  - Coordinating with Incident Management Coordinator to ensure timing is in accordance with regulatory requirements and that incident logging is complete for compliance evidence purposes

- Investigating Subject Matter Experts are responsible for detailed technical tasks related to the investigation of the incident and performing the needed recovery actions:
  - Perform investigation tasks related to the incident as assigned by the Incident Management Coordinator to determine the root cause of the incident
  - Perform service restoration tasks related to the incident as assigned
  - Update incident ticket and ensure all required details are logged
  - Obtaining information on the three required attributes for both initial notification and updates
  - After incident closure, participate in "Lessons Learned" sessions and update procedures as needed

Incident handling procedures for Cyber Security Incidents (R1.4)

Each of the defined roles in the example process may have specific procedures covering various aspects of their tasks being accomplished within the process. The sample process documents "what" the overall required steps are whereas the procedures document "how" each step is carried out:

- Incident Management Service Desk Procedures:
    - Procedures of when to classify cyber events as possible cyber incidents
    - Procedures to determine if BCS, PSP, ESP or EACMS are involved and decision criteria of when to escalate to an Incident Management Coordinator.
    - Procedures for initial diagnosis, triage and service restoration
    - Procedures for incident ticketing, assignment, escalation and closure

- Incident Management Coordinator Procedures:
    - Procedures for finding if cyber events or incidents could be possible Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. These potential incidents require notification to the E-ISAC/ NCCIC Coordinator
    - Procedures for the assignment and tracking of tasks to Investigating SMEs
    - Procedures associated with regulatory reporting time limits
    - Procedures for incident review, documentation of lessons learned, tracking of completion of documentation update status
- E-ISAC/ NCCIC Reporting Coordinator Procedures:
    - Procedures on how to use the Entity's own classification and reporting schema to classify cyber incidents and determine Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part
    - Procedures on the review of information to be used for reporting the three required attributes to be included for E-ISAC or NCCIC notification including the handling of any BES Cyber System Information
    - Procedures for the notification of updates to E-ISAC and NCCIC including the submission of the three required attributes
- Investigating Subject Matter Experts Procedures:
    - Procedures for the classification of cyber incidents to possible Cyber Security Incidents, possible Reportable Cyber Security Incidents or possible Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part and the required information needed to be obtained.
    - Procedures for troubleshooting tasks to determine root cause of an incident

- Procedures for service restoration tasks after an incident
- Procedures for triggering the forensic preservation of the incident
- Procedures on when updates are necessary to information on the required attributes associated with a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for the Part

Requirement R2

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]*

2.1. 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.

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.

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.

Applicable Systems for the three collective Parts in Requirement R2 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R2

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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, multi-discipline 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. 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.

[7] 2009, Department of Homeland Security, Developing an Industrial Control Systems Cybersecurity Incident Response Capability, page 13.

Requirement R3

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].*

3.1. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:

3.1.1. Document any lessons learned or document the absence of any lessons learned;

3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and

3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

3.2. No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:

3.2.1. Update the Cyber Security Incident response plan(s); and

3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.

Applicable Systems for the two collective Parts in Requirement R3 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R3

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

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.

Requirement R4

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].*

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

Applicable Systems for the three collective Parts in Requirement R4 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

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"

NCCIC Reporting

NCCIC reporting guidelines for reporting events related to Industrial Control Systems can be found here:

https://ics-cert.us-cert.gov/Report-Incident
https://www.us-cert.gov/incident-notification-guidelines

NCCIC prefers the reporting of 10 attributes, although they will accept any information that is shared. A potential mapping between the NCCIC preferred attributes and the attributes required to comply with CIP-008-6 standard could be represented are as follows:

CIP-008-6 Reporting	NCCIC Reporting	Comment
Functional Impact	Identify the current level of impact on agency functions or services (Functional Impact).	
Functional Impact	Identify the type of information lost, compromised, or corrupted (Information Impact).	
Functional Impact	Identify when the activity was first detected.	
Level of Intrusion	Estimate the scope of time and resources needed to recover from the incident (Recoverability).	
Level of Intrusion	Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident	
Level of Intrusion	Identify the number of systems, records, and users impacted.	
Level of Intrusion	Identify the network location of the observed activity.	
Level of Intrusion	Provide any mitigation activities undertaken in response to the incident.	
Attack Vector	Identify the attack vector(s) that led to the incident.	
Name and Phone	Identify point of contact information for additional follow-up.	

Figure 11 NCCIC Reporting Attributes

Example of a Reporting Form

Entities may wish to create an internal standard form to be used to report Reportable Cyber Security Incidents and Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The advantages of using a standard internal form are:

- A standard internal format for the communications of cyber incident information between the various internal roles with respect to obligations of CIP-008-6, Requirement R4
- A standard written record of the notification of the minimum 3 attributes having been reported to E-ISAC and NCCIC in accordance with CIP-008-6, Requirement R4 which can be easily stored, sorted and retrieved for compliance purposes

An example of an internal standard form is shown. The instructions on how to complete this form are included after it.

CIP-008-6 Requirement R4

Cyber Security Incident Reporting Form

This form may be used to report Reportable Cyber Security Incidents and Cyber Security Incidents that were an attempt to compromise a system listed in the "Applicable Systems" column for the Part.

Contact Information

Name: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

Click or tap here to enter text.

Instructions for Example of a Reporting Form

These are instructions on one way to complete the optional form.

CIP-008-6
Cyber Security Incident Reporting Form Instructions

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident. This field could also be used to identify the company name of the Registered Entity.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if report includes information for a Reportable Cyber Security Incident.
	Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Check this box if report includes information for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if report is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if report is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.3.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
	Attack Vector Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber System classification level.*
	Level of Intrusion Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If report is being used to provide an update, select the 'Update' checkbox.

Exhibit F

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Incident Report

Technical Rationale and Justification for Reliability Standard CIP-008-6

RELIABILITY | ACCOUNTABILITY



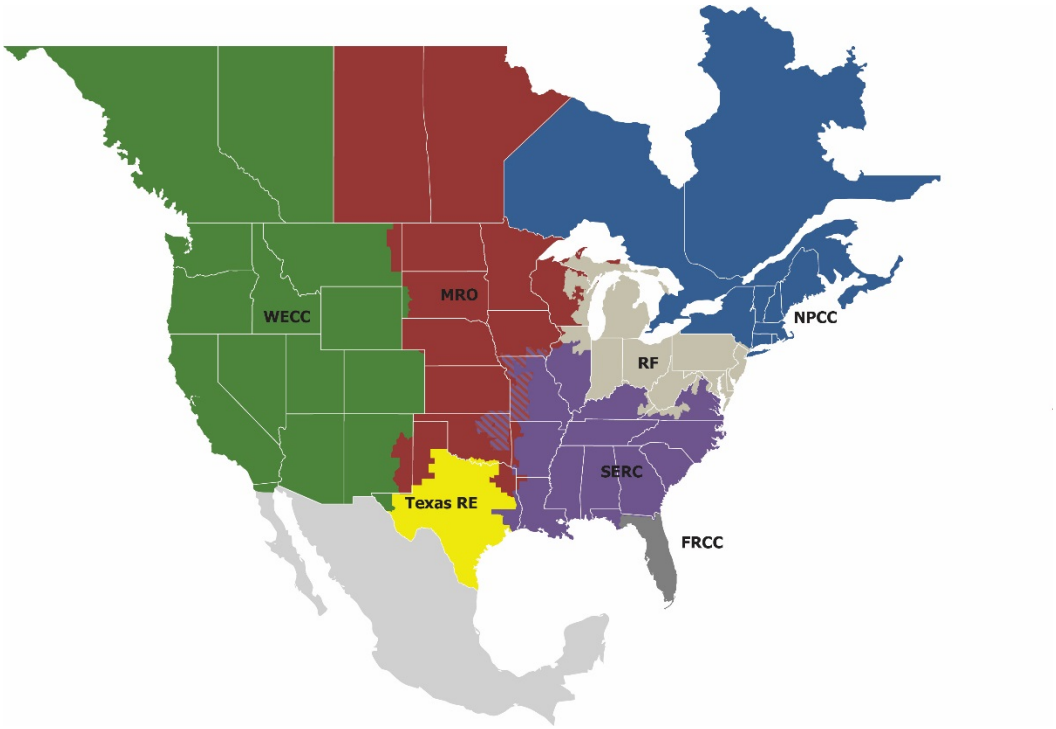

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards 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 and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

[1] 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).

New and Modified Terms Used in NERC Reliability Standards

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident

A Cyber Security Incident that 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 Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for "A BES Cyber System that performs one or more reliability tasks of a functional entity" to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

New and Modified Terms Used in NERC Reliability Standards

EACMS

The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "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 the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "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."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

Requirement R4

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Requirement R4

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-008-5 standard to preserve any historical references.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:
This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

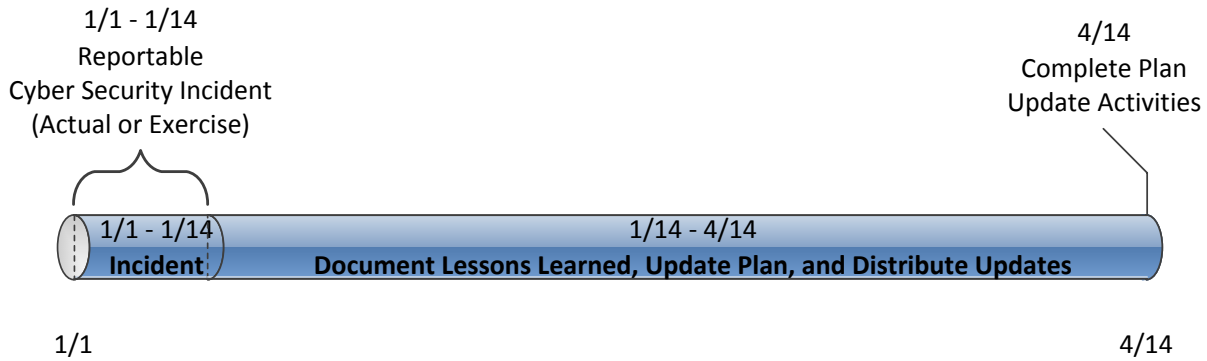
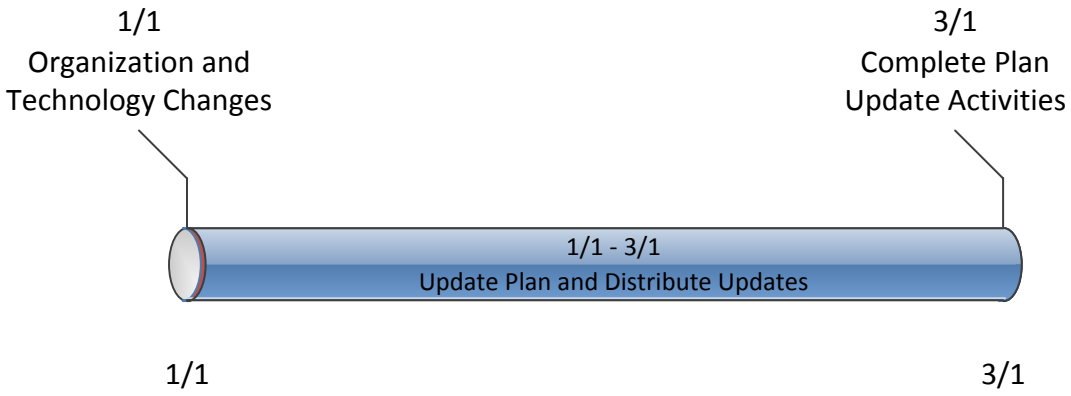


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

Exhibit G

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-008-6. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-008-6, Requirement R1
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R1
The justification is provided on the following pages.

VRF Justification for CIP-008-6, Requirement R2
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R2
The VSL did not substantively change from the previously FERC-approved CIP-008-5 Reliability Standard. Only minor revisions were made.

VRF Justification for CIP-008-6, Requirement R3
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R3
The VSL did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VRF Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSL Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSLs for CIP-008-6, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (1.2)

		criteria to evaluate and define attempts to compromise. (1.2)	

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from FERC-approved CIP-008-5 and add two VSLs to the High and Severe categories to reflect new subparts 1.2.1 and 1.2.3. The two new VSLs are similar to currently-approved VSLs. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The proposed VRF is consistent among other FERC approved VRF's within the standard.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The team relied on NERC's definition of lower risk requirement.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)		successors, of a Reportable Cyber Security Incident. (R4)	

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

Exhibit H

Summary of Development History and Complete Record of Development

Summary of Development History

Summary of Development History

The following is a summary of the development record for proposed Reliability Standard CIP-008-6.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team ("SDT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the SDT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2018-02 – Modifications to CIP-008 Cyber Security Incident Reporting SDT members is included in **Exhibit I**.

II. Standard Development History

A. Standard Authorization Request Development

Project 2018-02 – Modifications to CIP-008 Cyber Security Incident Reporting was initiated on March 9, 2016 as a Standards Authorization Request ("SAR") to address the Commission directive in Order No. 848.[3] On August 10, 2018, the Standards Committee Executive Committee accepted the SAR and authorized posting the SAR for a 30-day informal comment period from August 10, 2018 through September 10, 2018.

---

[1] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2012).

[2] The NERC *Standard Processes Manual* is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

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

B. First Posting - Comment Period, Initial Ballot and Non-binding Poll

Proposed Reliability Standard CIP-008-6, the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident, the associated Implementation Plan, Violation Risk Factors ("VRFs"), Violation Severity Levels ("VSLs"), and other associated documents were posted for a 20-day formal comment period from October 3, 2018 through October 22, 2018, with a parallel initial ballot and non-binding poll held during the last 5 days of the comment period from October 18, 2018 through October 22, 2018.[4] The initial ballot for proposed CIP-008-6 received 20.02 percent approval, reaching quorum at 81.17 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 23.2 percent supportive opinions, reaching quorum at 79 percent of the ballot pool. There were 86 sets of responses, including comments from approximately 176 different individuals and approximately 116 companies, representing all 10 industry segments.[5]

C. Second Posting - Comment Period, Additional Ballot and Non-binding Poll

Proposed Reliability Standard CIP-008-6, the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 15-day formal comment period from November 15, 2018 through November 29, 2018, with a parallel additional ballot as well as the non-binding poll held during the last 10 days of the comment period from November 20, 2018

---

[4] 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. The minutes from the Standards Committee meeting on September 13, 2018 are available at https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/Standards%20Committee%20Meeting%20Minutes-Approved%20October%2017,%202018.pdf.

[5] NERC, *Consideration of Comments*, Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting (Nov. 2018), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Consideration_of_Comments_Draft_11152018.pdf.

through November 29, 2018.[6] The additional ballot for CIP-008-6 reached quorum at 94.44 percent of the ballot pool and received 75.54 percent approval. The related non-binding poll for CIP-008-6 reached quorum at 93 percent of the ballot pool and received 75.81 percent supportive opinions. There were 72 sets of responses, including comments from approximately 160 different individuals and approximately 110 companies, representing seven of the 10 industry segments.[7]

D. Final Ballot

Proposed Reliability Standard CIP-008-6 was posted for an 8-day final ballot period from January 15, 2019 through January 22, 2019. The ballot for proposed Reliability Standard CIP-008-6 and associated documents reached quorum at 96.3 percent of the ballot pool, receiving support from 77.89 percent of the voters.

E. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standard CIP-008-6 on February 7, 2019.[8]

---

[6] 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. The minutes from the Standards Committee meeting on September 13, 2018 are available at https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/Standards%20Committee%20Meeting%20Minutes-Approved%20October%2017,%202018.pdf.

[7] NERC, *Consideration of Comments*, Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Consideration_of_Comments_Final%20Ballot_01152019.pdf.

[8] NERC, *Board of Trustees Agenda Package*, Agenda Item 6c (CIP-008-6 – Cyber Security – Incident Reporting and Response Planning) *available at* https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_of_Trustees_Open_Meeting_Agenda_Package-February_7_2019.pdf.

Complete Record of Development

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Related Files

Status
The **8-day** final ballot for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** concluded **8 p.m. Eastern, Tuesday, January 22, 2019.** The voting results can be accessed via the link below. The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)."

Standard(s) Affected – CIP-008-5

Project Scope
The Reliability Standard(s) developed or revised will include the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;

2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;

3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and

4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-008-6 Clean **(36)** | Redline to Last Posted **(37)** | Redline to Last Approved **(38)** Implementation Plan Clean **(39)** | Redline to Last Posted **(40)**	Final Ballot Info **(46)** Vote	01/15/19 - 01/22/19	Ballot Results **(47)**	

Supporting Materials VRF/VSL Justification Clean **(41)** | Redline to Last Posted **(42)** Technical Rationale **(43)** Implementation Guidance **(44)** Reliability Standard Audit Worksheet **(45)**				
Draft 2 CIP-008-6 Clean **(20)** | Redline to Last Posted **(21)** Implementation Plan Clean **(22)** | Redline to Last Posted **(23)** **Supporting Materials** Unofficial Comment Form (Word) **(24)** VRF/VSL Justifications Clean **(25)** | Redline to Last Posted **(26)** Technical Rationale **(27)** Implementation Guidance **(28)**	Additional Ballot and Non-binding Poll Updated Info **(29)** Info **(30)** Vote	11/20/18 - 11/29/18	Ballot Results **(31)** Non-binding Poll Results **(32)**	
	Comment Period Info **(33)** Submit Comments	11/15/18 - 11/29/18	Comments Received **(34)**	Consideration of Comments **(35)**
Draft 1 CIP-008-6 Clean **(6)** | Redline to Last Approved **(7)** Implementation Plan **(8)** **Supporting Materials** Unofficial Comment Form (Word) **(9)** VRF/VSL Justification **(10)** Consideration of Issue and Directives **(11)** Technical Rationale **(12)**	Initial Ballot and Non-binding Poll Updated Info **(13)** Info **(14)** Vote	10/18/18 - 10/22/18	Ballot Results **(15)** Non-binding Poll Results **(16)**	
	Comment Period Info **(17)** Submit Comments	10/03/18 - 10/22/18	Comments Received **(18)**	Consideration of Comments **(19)**
	Join Ballot Pools	10/03/18 - 10/17/18		

Standard Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(4)**	Nomination Period Info **(5)** Submit Nominations	08/10/18 - 08/29/18		
Standard Authorization Request **(3)** **Supporting Materials** Unofficial Comment Form (Word) **(1)**	Comment Period Info **(2)** Submit Comments	08/10/18 - 09/10/18		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting Standard Authorization Request

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting Standard Authorization Request (SAR)**. Comments must be submitted by **8 p.m. Eastern, Monday, September 10, 2018.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)."

The Reliability Standard(s) developed or revised will include the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

2. Provide any additional comments for the Standrds Drafting Team to consider, if desired.

   Comments:

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Informal Comment Period Open through September 10, 2018

Now Available

An informal comment period for the **Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting Standard Authorization Request** is open through **8 p.m. Eastern, Monday, September 10, 2018**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues using the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day.***

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Revisions to CIP-008-5 Cyber Security- Incident Reporting and Response Planning		
Date Submitted:	August 6, 2018		
SAR Requester			
Name:	Soo Jin Kim		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@nerc.net
SAR Type (Check as many as apply)			
☒ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☒ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☐ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
On July 19, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 848 in order to augment the mandatory reporting of Cyber Security Incidents.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." NERC was directed to submit the modifications within 6 months of the effective date of the final order.			

Requested information
Project Scope (Define the parameters of the proposed project):
The Standards Drafting Team (SDT) for Project 2018-02 will address FERC's directives in Order No. 848 that require developing or modifying existing Reliability Standards and associated definitions to augment the reporting of Cyber Security Incidents. The scope of any new reporting requirement will be tailored to provide better information on cyber security threats and vulnerabilities without imposing an undue burden on responsible entities.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
The SDT shall address the Order No. 848 directives. The Reliability Standard(s) developed or revised will include the 4 elements outlined by FERC: 1. responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; 2. required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; 3. establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and 4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). With regard to identifying EACMS for reporting purposes, the Commission stated that the reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. The Commission specified that, at a minimum, those functions must include: 1. authentication; 2. monitoring and logging; 3. access control; 4. interactive remote access; and 5. alerting.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
With regard to the definition of "attempted compromise" for reporting purposes, the Commission stated that it considers attempted compromise to include unauthorized access attempts or other confirmed suspicious activity. With regard to content to be included in each report, the Commission stated that the minimum set of attributes to be reported must include: 1. The 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.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
No additional cost outside of the time and resources needed to serve on the Standard Drafting Team are expected. However, a question will be asked during the SAR comment period to ensure all aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
None
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
No consensus building has been completed to date.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?
Project 2016-02 is currently working on addressing FERC directives and the V5TAG Transition document which include potential modifications to the ESP and EACMS definitions.
Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

NA

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
NA	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☒ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting Standard Drafting Team

Do not use this form for submitting nominations. Use the electric form to submit nominations for **Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting** standard drafting team (SDT) members by **8 p.m. Eastern, Wednesday, August 29, 2018.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Cyber Security Incident Reporting

The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)."

The Reliability Standard(s) developed or revised will include the 4 elements outlined by FERC:

1. responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Standard affected: CIP-008-5

A significant time commitment is expected of SDT members to meet the six-month regulatory deadline established in Order No. 848. SDT activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately three face-to-face meetings between September and December 2018 (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Due to the expedited timeline on this project, please be prepared for an initial meeting at the end of September 2018. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas:

- Critical Infrastructure Protection ("CIP") family of Reliability Standards
- Incident reporting
- Cyber Asset and BES Cyber Asset definitions
- Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	
Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):	
If you are currently a member of any NERC drafting team, please list each team here: ☐ Not currently on any active drafting team. ☐ Currently a member of the following drafting team(s):	
If you previously worked on any NERC drafting team please identify the team(s): ☐ No prior NERC drafting team. ☐ Prior experience on the following team(s):	

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:		
☐ Texas RE	☐ NPCC	☐ WECC
☐ FRCC	☐ RF	☐ NA – Not Applicable
☐ MRO	☐ SERC	

	Select each Industry Segment that you represent:
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Nomination Period Open through August 29, 2018

Now Available

Nominations are being sought for standard drafting team (SDT) members through **8 p.m. Eastern, Wednesday, August 29, 2018**.

Use the electronic form to submit a nomination. If you experience issues using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

A significant time commitment is expected of SDT members to meet the six-month regulatory deadline established in Order No. 848. SDT activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately three face-to-face meetings between September and December 2018 (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Due to the expedited timeline on this project, please be prepared for an initial meeting at the end of September 2018. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas:

- Critical Infrastructure Protection ("CIP") family of Reliability Standards
- Incident reporting
- Cyber Asset and BES Cyber Asset definitions
- Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Previous drafting or periodic review team experience is beneficial, but not required. See the project page and unofficial nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the team mid-September 2018. Nominees will be notified shortly after they have been selected.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 20-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018

Anticipated Actions	Date
20-day formal comment period with ballot	October 2018
15-day formal comment period with additional ballot	November 2018
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms:

Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Physical Security Perimeter or, (3) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Proposed New Term:

Reportable Attempted Cyber Security Incident:
A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident or a Reportable Attempted Cyber Security Incident and requires notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents and documented processes for notification.
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Reportable Attempted Cyber Security Incident, 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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Retain records related to Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

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].*

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.*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and each United States Responsible Entity also shall notify the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), or their successors, of Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents, unless prohibited by law, according to 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].*

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.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 1. The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ICS-CERT in the form of Attachment 1 submissions.

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Responsible Entities shall use one of the following methods for initial notification: • Electronic submission of Attachment 1; • Phone; or • Email. If Attachment 1 was not submitted for initial notification, it must be submitted within 5 calendar days of initial notification, without attribute information if undetermined at the time of submittal.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of electronic submissions of Attachment 1, phone records or email.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Timeline for initial notification: • One hour from the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of phone records for preliminary notice or submissions through the E-ISAC and ICS-CERT approved methods, or Attachment 1 submissions.

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Responsible Entities shall submit Attachment 1 updates for the attributes required in Part 4.1 within 5 calendar days of determination of new or changed attribute information. Submissions must occur each time new attribute information is available until all attributes have been reported.	Examples of evidence may include, but are not limited to, dated documentation of Attachment 1 submissions to the E-ISAC and ICS-CERT.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role	120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to	The Responsible Entity failed to notify E-ISAC or ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4) OR The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2.	of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4) OR The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.	Requirement R4, Part 4.3.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2018-02. A separate technical rationale document has been created to cover Project 2018-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. 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, multi-discipline 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*. 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.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

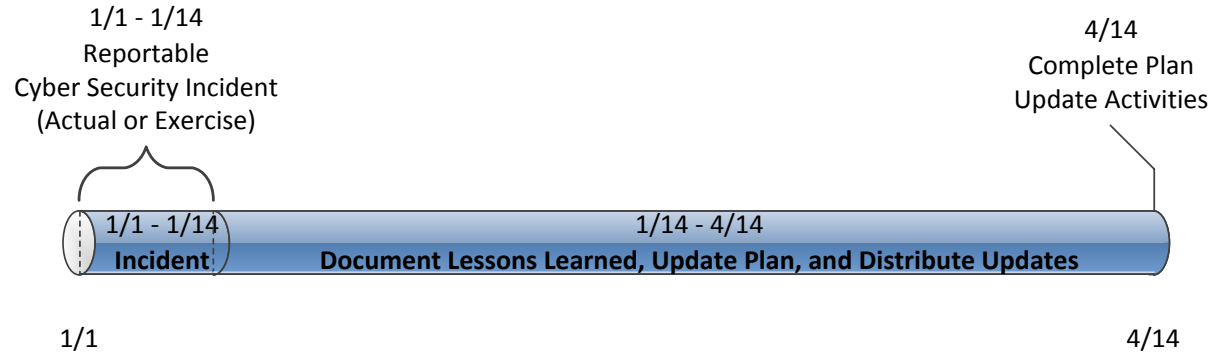


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. 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.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

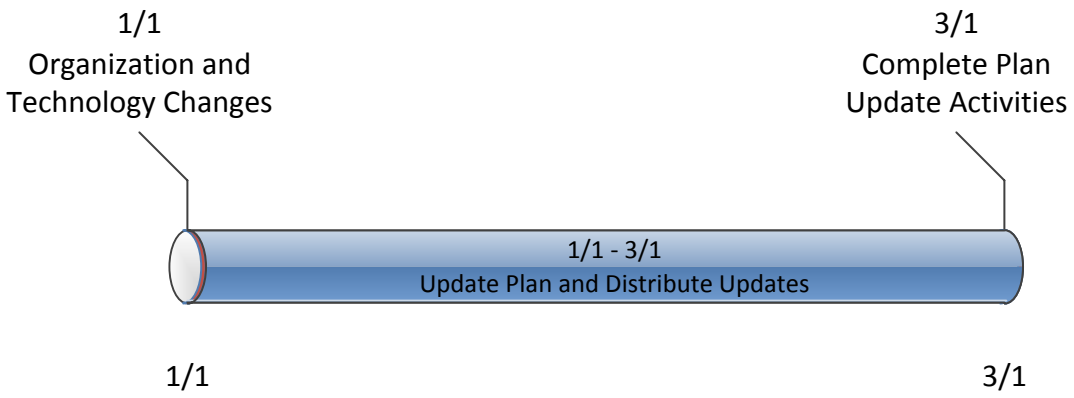


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. 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.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	10/4/18	Modified to address directives in FERC Order No. 848	

CIP-008-6 - Attachment 1

Cyber Security Incident Reporting Form

Use this form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents in accordance with CIP-008-6, Requirement R4.

Contact Information

Name:	Click or tap here to enter text.
Phone Number:	Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Reportable Attempted Cyber Security Incident

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

   Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

   Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

CIP-008-6 - Attachment 2

Cyber Security Incident Reporting Form Instructions

Attachment 2 provides instructions to aid in the completion of Attachment 1.

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if Attachment 1 includes information for a Reportable Cyber Security Incident.
	Reportable Attempted Cyber Security Incident	Check this box if Attachment 1 includes information for a Reportable Attempted Cyber Security Incident. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if Attachment 1 is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if Attachment 1 is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.2.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*
	Attack Vector Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber Asset classification level.*
	Level of Intrusion Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of proposed standard for formal 20-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018

Anticipated Actions	Date
20-day formal comment period with ballot	October 2018
15-day formal comment period with additional ballot	November 2018
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms:

Cyber Security Incident:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Physical Security Perimeter or, (3) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident:

A Cyber Security Incident that has compromised or disrupted:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Proposed New Term:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

~~B.~~

~~C.~~A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-65

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-~~6~~5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.~~1. **24 Months Minimum –** CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

6. Background:

Standard CIP-008~~-5~~ exists as part of a suite of CIP Standards related to cyber security. CIP-002~~-5~~ requires the initial identification and categorization of BES Cyber Systems. CIP-003~~-5~~, CIP-004~~-5~~, CIP-005~~-5~~, CIP-006~~-5~~, CIP-007~~-5~~, CIP-008~~-5~~, CIP-009~~-5~~, CIP-010~~-1~~, and CIP-011~~-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002~~-5~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002~~-5~~ identification and categorization processes.

~~D.~~B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident ~~and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 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.~~or a Reportable Attempted Cyber Security Incident and requires notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents ~~and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).~~ or Reportable Attempted Cyber Security Incidents and documented processes for notification.
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Reportable Attempted Cyber Security Incident, 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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Retain records related to Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

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].*

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*.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and each United States Responsible Entity also shall notify the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), or their successors, of Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents, unless prohibited by law, according to 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].*

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.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 1. The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ICS-CERT in the form of Attachment 1 submissions.

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Responsible Entities shall use one of the following methods for initial notification: • Electronic submission of Attachment 1; • Phone; or • Email. If Attachment 1 was not submitted for initial notification, it must be submitted within 5 calendar days of initial notification, without attribute information if undetermined at the time of submittal.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of electronic submissions of Attachment 1, phone records or email.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Timeline for initial notification: • One hour from the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of phone records for preliminary notice or submissions through the E-ISAC and ICS-CERT approved methods, or Attachment 1 submissions.

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Responsible Entities shall submit Attachment 1 updates for the attributes required in Part 4.1 within 5 calendar days of determination of new or changed attribute information. Submissions must occur each time new attribute information is available until all attributes have been reported.	Examples of evidence may include, but are not limited to, dated documentation of Attachment 1 submissions to the E-ISAC and ICS-CERT.

~~E.~~C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-65)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents. (1.2) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)~~
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Reportable Attempted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Security Incident or Reportable Attempted Cyber Security Incident occurs. (2.2)	Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or	response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.		
R4	Operations Assessment	Lower	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4) OR The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4) OR The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3.	The Responsible Entity failed to notify E-ISAC or ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2.	Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.		

~~F.~~D. Regional Variances

None.

~~G.~~E. Interpretations

None.

~~H.~~F. Associated Documents

None.

Guidelines and Technical Basis

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2018-02. A separate technical rationale document has been created to cover Project 2018-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. 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, multi-discipline 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*. 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.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

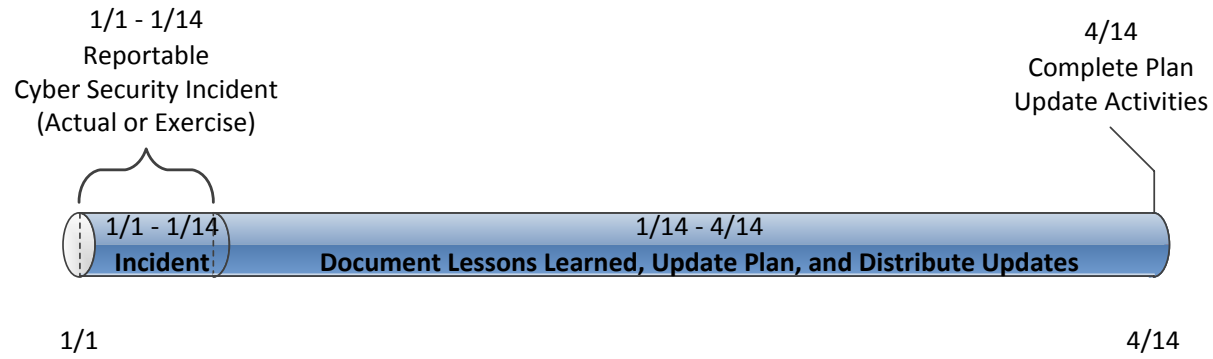


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. 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.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

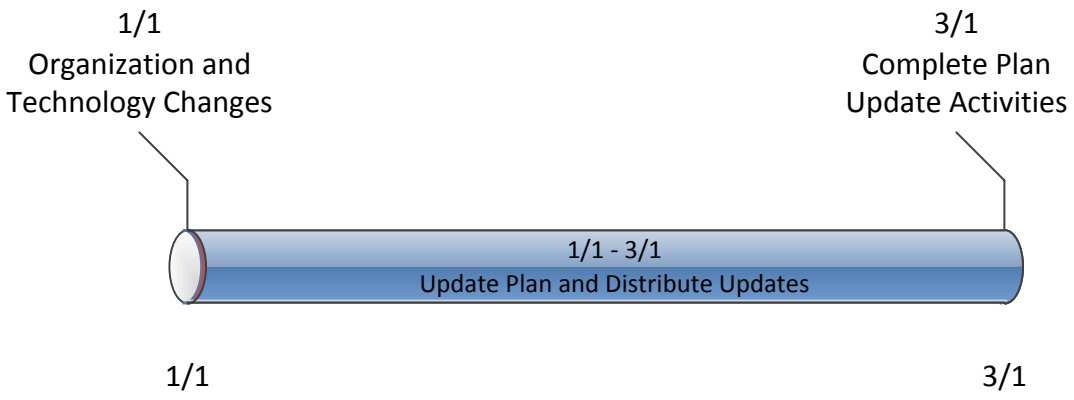


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. 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.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	10/4/18	Modified to address directives in FERC Order No. 848	

CIP-008-6 - Attachment 1

Cyber Security Incident Reporting Form

Use this form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents in accordance with CIP-008-6, Requirement R4.

Contact Information	
Name:	Click or tap here to enter text.
Phone Number:	Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Reportable Attempted Cyber Security Incident

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

CIP-008-6 - Attachment 2

Cyber Security Incident Reporting Form Instructions

Attachment 2 provides instructions to aid in the completion of Attachment 1.

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if Attachment 1 includes information for a Reportable Cyber Security Incident.
	Reportable Attempted Cyber Security Incident	Check this box if Attachment 1 includes information for a Reportable Attempted Cyber Security Incident. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if Attachment 1 is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if Attachment 1 is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.2.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*
	Attack Vector Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber Asset classification level.*
	Level of Intrusion Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

Requested Retirement

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New Terms in the NERC Glossary of Terms

This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Proposed New Definition:
Reportable Attempted Cyber Security Incident:
A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or

- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Proposed Modified Definitions:
Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter, (2) or Physical Security Perimeter, or (3) Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems, or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Proposed Retirements of Approved Definitions:
Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Background

The purpose of this project is to address the directives issued by FERC in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Effective Date

Reliability Standard CIP-008-6
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 12 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 12 calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Definition
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 12 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 12 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.

Retirement Date

Reliability Standard CIP-008-5
Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Definition

The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Note that this comment period is 20 days, with the ballot pool forming the first 15 and the initial ballot conducted the final 5 days.

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to provide comments on **CIP-008-6 — Cyber Security - Incident Reporting and Response Planning**. Comments must be submitted by **8 p.m. Eastern, Tuesday, October 22, 2018.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Questions

1. The Standard Drafting Team (SDT) created a new definition and modified existing definitions to address the directive in FERC Order No. 848 paragraph 31 regarding "attempts to compromise" without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use existing *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary) definitions. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident, and the proposed new definition of, Reportable Attempted Cyber Security Incident? If not, please provide comments and alternate language, if possible.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? If not, please provide comments and an alternate approach to addressing the directive, if possible.

   ☐ Yes
   ☐ No

   Comments:

3. Do you agree with reporting timeframes included Requirement R4? If you disagree please explain and provide alternative language and rationale for how it meets the directives in FERC Order No. 848.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT created Attachment 1 to be used for consistent reporting and intentionally aligned the content with FERC Order No. 848 paragraphs 69 and 73. Do you agree with the content and use of Attachment 1?

   ☐ Yes
   ☐ No

   Comments:

5. Do you agree with the required methods of notification proposed by the SDT in Requirement R4, Part 4.2? If no, please explain and provide comments.

   ☐ Yes
   ☐ No

   Comments:

6. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R4? If no, please explain and provide comments.

   ☐ Yes
   ☐ No

   Comments:

7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

8. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

9. Provide any additional comments for the SDT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in [Project Number and Name or Standard Number]. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. The VRF is being established for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The proposed VRF is consistent among other FERC approved VRF's within the standard.
FERC VRF G4 Discussion	The team relied on NERC's definition of lower risk requirement.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
Guideline 4- Consistency with NERC Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4) OR The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4) OR	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3.	The Responsible Entity failed to notify E-ISAC or ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2.	The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.		

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Augment reporting to include Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems	FERC Order 848, p3	The Project 2018-02 Standard Drafting Team (SDT) agrees that Reliability Standards include mandatory reporting of Cyber Security Incidents that compromise or attempt to compromise a Responsible Entities Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems and therefore proposes modification of NERC Glossary of Terms definitions for Cyber Security Incident and Reportable Cyber Security Incident and proposes the addition of EACMS associated with High and Medium BES Cyber Systems as applicable systems for requirements CIP-008 R1, R2, R3, and R4.
Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Specifically, the minimum set of attributes to be reported should include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or	FERC Order 848, p3 and p13	The SDT agrees that Cyber Security Incident reports should include certain minimum information detailed in FERC Oder 848 p3 and p13 to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. The SDT drafted CIP-008 R4 to address those minimum set of attributes to include; (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or attempt to achieve the Cyber Security

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
attempt to achieve the Cyber Security Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident.		Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident. Additionally, the SDT is requiring the use of Attachment 1, Cyber Security Incident Reporting Form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents which includes required minimum attributes. This requirement and use of a standardized reporting form will ensure required information is reported in consistent manner improving the quality of reporting.
Filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a Responsible Entity	FERC Order 848, p3	The SDT agrees that the filing deadlines for Cyber Security Incident Reports should be established as identified in FERC Order 848, paragraph 3. The SDT proposes the addition of CIP-008 Requirement 4 to establish report filing deadlines for a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, once it is determined by a Responsible Entity.
Reports should continue to be sent to the E-ISAC, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	FERC Order 848, p3	The SDT agrees that reports should be submitted to the E-ISAC, and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and proposes the addition of CIP-008 Requirement 4 to establish reporting obligations. Requirement 4 includes the requirement to notify E-ISAC and ICS-CERT using a method identified in the requirement part such as submitting Attachment 1 via email or via the E-ISAC and ICS-CERT portals. The SDT did not modify any language that would remove or

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		alter the obligation to report to DHS through EOP-004 or OE-417.
With regard to identifying EACMS for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting. Reporting a malicious act or suspicious event that has compromised, or attempted to compromise, a responsible entity's EACMS that perform any of these five functions would meet the intended scope of the directive by improving awareness of existing and future cyber security threats and potential vulnerabilities. In a similar vein, the assets (i.e., EACMS) subject to the enhanced reporting requirements should be identified based on function, as opposed to a specific technology that could require a modification in the reporting requirements should the underlying technology change.	FERC Order 848, p54 and p70	The SDT agrees that for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. The proposed new definition, Reportable Attempted Cyber Security Incident, identifies Cyber Security Incidents that attempt to compromise or disrupt any of the following EACMS functions related to electronic access: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting, as listed in FERC Order 848, paragraph 54 and 70.
With regard to timing, we conclude that NERC should establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT based on a risk impact assessment and incident prioritization approach to incident reporting.	FERC Order 848, p89	The SDT agrees that reporting timelines should be established for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT based on a risk impact assessment, as identified in FERC order 848, paragraph 89. The SDT proposes the addition of CIP-008 Requirement 4 to

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
This approach would 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.		establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT. The initial notification timelines are identified in the proposed Requirement 4, Part 4.3, and the update timelines are identified in the proposed Requirement 4, Part 4.4. The proposed reporting timelines 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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Report

Technical Rationale and Justification for Reliability Standard CIP-008-6

October 2018

RELIABILITY | ACCOUNTABILITY



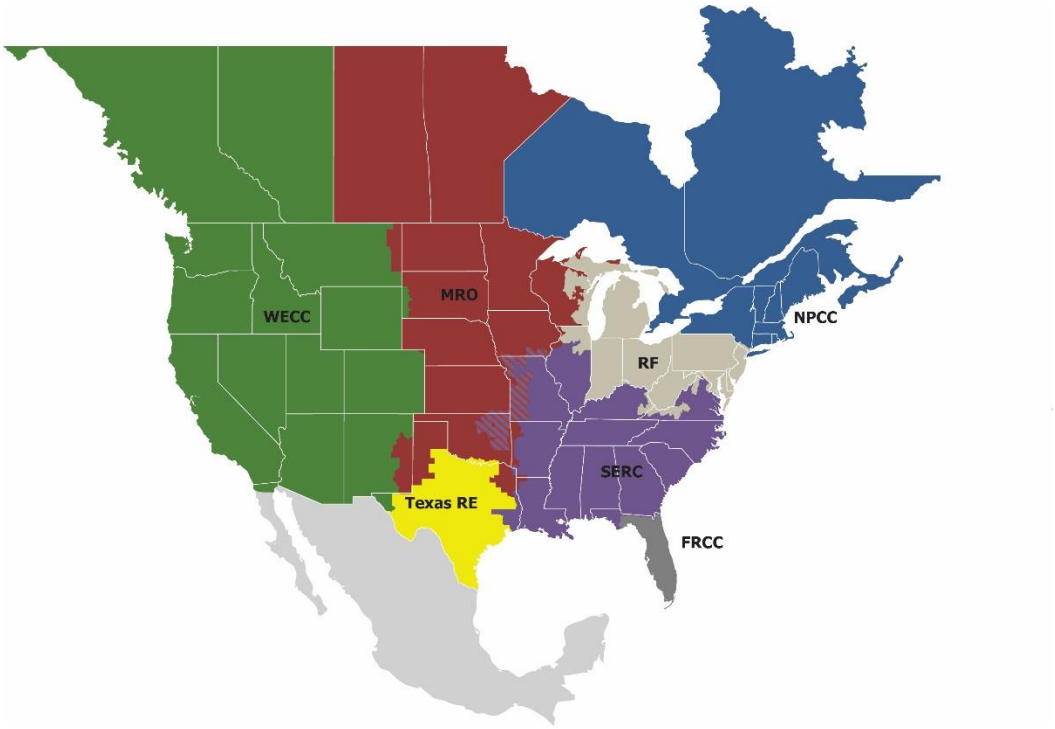

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848, where the FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards 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 and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)

New and Modified Terms Used in NERC Reliability Standards

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter, (2) or Physical Security Perimeter, or (3) Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.*

The SDT modified the Cyber Security Incident definition to add part (3), above, to include Electronic Access Control or Monitoring Systems (EACMS) in response to the Order. FERC Order 848, Paragraph 1, directs the modification of the Reliability Standards to require the reporting of Cyber Security Incidents to include the responsible entity's ESP(s) (already included above) or associated EACMS (which the SDT added to the above definition).

The SDT considered potential unintended consequences related to the use of the existing definition in CIP-003-6 and qualified the addition of Electronic Access Control or Monitoring Systems with '*High or Medium Impact BES Cyber Systems'* to assure clarity and the SDT's intentions to exclude low impact.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted:

- *One or more reliability tasks of a functional entity; or*
- *Electronic Security Perimeter; or*
- *Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting*

The SDT also modified the Reportable Cyber Security Incident definition to comply with FERC Order 848. The SDT modified the Reportable Cyber Security Incident definition to include incidents that compromised or disrupted an ESP or an EACMS that provides specific functions, as directed by the Order. (Order 848, Paragraph 54)

The SDT considered potential unintended consequences related to the use of the existing definition in CIP-003-6 and qualified the addition of Electronic Access Control or Monitoring Systems with '*High or Medium Impact BES Cyber Systems'* to assure clarity and the SDT's intentions to exclude low impact.

Proposed New Term:

Reportable Attempted Cyber Security Incident

A Cyber Security Incident that was an attempt to compromise or disrupt:

- *One or more reliability tasks of a functional entity; or*
- *Electronic Security Perimeter; or*
- *Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting*

The SDT created this new definition to clarify attempted Cyber Security Incidents subject to reporting. FERC Order 848 specifically directs modifying the Reliability Standard(s) to require reporting of attempted compromises for ESP(s) or associated EACMS(s). The SDT included the list of EACMS functions to clarify the parameters of Reportable Attempted Cyber Security Incidents related to EACMS.

The Order specifically required the reporting of attempts to compromise for ESP, and EACMS, the SDT included "One or more reliability tasks of a functional entity in the definition to be consistent with Reportable Cyber Security Incidents.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, which directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 while also addressing the required changes, thus the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1 the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted the Requirement R1 Part 1.2 reporting requirements and moved them to Requirement R4 to serve this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has recently begun to change its name to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems, and the E-ISAC has previously re-branded their name and may again in the future. By following Requirement R4 references to E-ISAC and ICS-CERT with "or their successors" the SDT intended to ensure Requirement R4 can be implemented even if the names of E-ISAC and ICS-CERT change or a different agency take over their current role.

Reported Attempted Cyber Security Incidents not eligible to meeting testing requirement

Requirement R2 Part 2.1 requires a test of the responsible entity's incident response plan for a Reportable Cyber Security Incident. The SDT debated whether testing incident response plans for a Reportable Attempted Cyber Security Incident would also meet the Requirement R2 Part 2.1 testing requirement. However, the SDT concluded that testing only the parts of a responsible entity's incident response plan required to respond to an attempt to compromise applicable Cyber Systems would not subject the testing to the same rigor as a response to an actual compromise.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and newly-defined Reportable Attempted Cyber Security Incidents (refer to Proposed New Term, above). Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification, thus added "to the extent known" to account for this scenario.

Methods for Submitting Notifications

Requirement R4 Part 4.2 specifies responsible entities shall use one of three methods for initial notification. The SDT endeavored to provide latitude in reporting methods and format for initial notification, to allow responsible entities' personnel to focus on incident response itself and not methods and format of reporting in this stage of incident response. The SDT defined three initial notification methods to provide a measure of standardization industry-wide. While Requirement R4 Part 4.2 allows for several methods of initial notification, it also requires submission of Attachment 1 to facilitate standardized reporting.

- *Electronic submission of Attachment 1* – The SDT envisions this as a simple email with Attachment 1 attached. However, the requirement is written to be broad enough that should either E-ISAC or ICS-CERT, or their successors, offer other options for submitting Attachment 1 like a web portal, this would still be within the requirement language.
- *Phone* – The SDT sees notification via telephone as a reasonable format for initial notification as it is quick and allows personnel to get back to incident response expeditiously.
- *Email* – In this context, a manually populated or automatically generated email can be submitted by simply including the required attributes without any specific format directly in an email to E-ISAC and ICS-CERT, or their successors. Again, the SDT views this as a quicker reporting method that could be used as a preliminary method to notify during incident response.

The last paragraph of the requirement was included to ensure that known data in a common format is eventually submitted via Attachment 1, as a common form allows for easier summarization, correlation, and trending of events.

Notification Timing

Requirement R4 Part 4.3 specifies two timelines for notification submission: one hour for Reportable Cyber Security Incidents and end of next calendar day for Reportable Attempted Cyber Security Incidents. FERC Order No 848 directly states that reporting deadlines must be established in paragraph 3, and later in paragraph 89 states that "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."

- *Reportable Cyber Security Incidents* – The SDT wrote Part R4.3 to use a one hour deadline for reporting of these events, as incidents in this category include successful penetrations of ESPs, EACMS or BES Cyber Systems. One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.

Requirement R4

- *Reportable Attempted Cyber Security Incidents* – Due to the lower severity of these unsuccessful attempts at penetrating ESP(s), EACMS, or BES Cyber Systems, the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day (11:59 pm local time)" was to afford responsible entities additional time to gather facts prior to notifications for the less severe Reportable Attempted Cyber Security Incident category.
- *Initial* submission may be by made by one of the three methods described above. The SDT understands that initial notification may not have all the details, but when Attachment 1 or an email is submitted, it is expected that information that has been determined is reported within the notification deadlines.

Notification Updates

Requirement R4 Part 4.4 requires that responsible entities shall submit Attachment 1 updates for the required attributes upon determination of new or changed attribute information. The SDT added this language to provide responsible entities sufficient time to determine attribute information, which may be unknown at the time of initial notification and which may change as more information is gathered. The intent of Requirement R4 Part 4.4 is to provide a method for responsible entities to report new information over time as investigations progress. NOTE: The SDT does not intend Attachment 1 updates specified in Requirement R4. Part 4.4 to expose responsible entities to potential violations if, for instance, an initial notification on an attribute and an updated notification on the same attribute have different information, since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.4 is to have a mechanism to report incident information to E-ISAC and ICS-CERT, or their successors, (and therefore, industry) upon determination of each required attribute.

Attachment 1

General Considerations for Attachment 1

As discussed above in Requirement R4 rationale, the SDT created Attachment 1 to provide a standard method for reporting to both E-ISAC and ICS-CERT or their successors until a time comes where an online portal may be developed. Since the Order directs requiring reporting to both agencies, a standard format will allow responsible entities to complete a single form and submit it to both agencies. (Order 848, Paragraph 3)

There was debate among the SDT on what to include in Attachment 1, and the SDT decided to include only those elements required by FERC Order 848, to assure required attributes are captured and minimize risk of possible violations for the responsible entities submitting the form. The SDT discussed potentially proposing modifications to DOE Form OE-417 to meet the directives in the Order, however, with the recent updates of OE-417 by DOE and timing of the Order, the SDT determined there was not enough time to make those modifications. The SDT interpreted that FERC did not support the use of OE-417, since the Order notes the differences of DOE's definition of a "Cyber Event" and NERC's definition of a Cyber Security Incident. (Order 848, Paragraph 73) Additionally, the SDT had concerns that OE-417 was designed for a different purpose and considered the use of this form for CIP-008 reporting to be inefficient for reporting only the required attributes.

The SDT was purposeful in the design of Attachment 1 to be concise and require limited data. The intent was to ease the burden on responsible entities by providing a method to quickly report required data while protecting entities from concerns with over-reporting and potentially exposing protected information under CIP-004 and CIP-011.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Initial Ballot and Non-ballot Poll Open through October 22, 2018

Now Available

The initial ballot and non-binding poll for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** are open through **8 p.m. Eastern, Monday, October 22, 2018.**

Balloting

Members of the ballot pools associated with this project can log into the Standards Balloting and Commenting System (SBS) and submit their votes. If you experience issues using the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Formal Comment Period Open through October 22, 2018
Ballot Pools Forming through October 17, 2018

Now Available

A 20-day formal comment period for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** is open through **8 p.m. Eastern, Monday, October 22, 2018.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues using the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Wednesday, October 17, 2018.** Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

A 5-day initial ballot for the standard, and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **October 18-22, 2018**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/156)
Ballot Name: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 IN 1 ST
Voting Start Date: 10/18/2018 12:01:00 AM
Voting End Date: 10/22/2018 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 263
Total Ballot Pool: 324
Quorum: 81.17
Weighted Segment Value: 20.02

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	90	1	16	0.225	55	0.775	0	1	18
Segment: 2	7	0.7	0	0	7	0.7	0	0	0
Segment: 3	72	1	9	0.158	48	0.842	0	1	14
Segment: 4	18	1	4	0.286	10	0.714	0	0	4
Segment: 5	74	1	14	0.25	42	0.75	0	2	16

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	53	1	10	0.222	35	0.778	0	1	7
Segment: 7	1	0.1	0	0	1	0.1	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	0	0	1	0.1	0	0	0
Segment: 10	8	0.3	1	0.1	2	0.2	0	3	2
Totals:	324	6.2	54	1.241	201	4.959	0	8	61

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		None	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Beaches Energy Services	Don Cuevas	Brandon McCormick	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Laura Lee		None	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Gainesville Regional Utilities	David Owens	Brandon McCormick	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Third-Party Comments
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		None	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	William Sanders		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Mike Smith		Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Nathaniel Clague		None	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Negative	Comments Submitted
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz	Dennis Chastain	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Douglas Webb	Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas		Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Terry BIlke		Negative	Comments Submitted
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Leanna Lamatrice		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Vo	Gary Nolan	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		None	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Brandon McCormick	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Negative	Third-Party Comments
3	Intermountain REA	David Maier		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lakeland Electric	Patricia Boody		Negative	Third-Party Comments
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand	Scott Miller	None	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen	Brandon McCormick	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	Aaron Smith		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
3	Rutherford EMC	Tom Haire		Negative	Third-Party Comments
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		None	N/A
3	Santee Cooper	James Poston		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		Negative	Comments Submitted
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	None	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Negative	Third-Party Comments
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Westar Energy	Bryan Taggart	Douglas Webb	Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Negative	Third-Party Comments
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		None	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Negative	Third-Party Comments
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Michael Brytowski	Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		None	N/A
5	JEA	John Babik		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	MEAG Power	Steven Grego	Scott Miller	None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NaturEner USA, LLC	Eric Smith		None	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Brett Jacobs		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Affirmative	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Mark McDonald		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Vistra Energy	Dan Roethemeyer		Negative	Third-Party Comments
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Westar Energy	Derek Brown	Douglas Webb	Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Nicholas Kirby		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Negative	Third-Party Comments
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Kris Butler		Negative	Comments Submitted
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Modesto Irrigation District	James McFall	Courtney Lowe	None	N/A
6	Muscatine Power and Water	Ryan Streck		None	N/A
6	New York Power Authority	Thomas Savin	Shelly Dineen	Negative	Third-Party Comments
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted
6	Portland General Electric Co.	Daniel Mason		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		Negative	Comments Submitted
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	SCANA - South Carolina Electric and Gas Co.	John Folsom		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		None	N/A
6	Westar Energy	Grant Wilkerson	Douglas Webb	Negative	Comments Submitted
6	Western Area Power Administration	Charles Faust		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Luminant Mining Company LLC	Brenda Hampton		Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Third-Party Comments
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Drew Slabaugh		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 324 of 324 entries

BALLOT RESULTS

Ballot Name: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 Non-binding Poll IN 1 NB
Voting Start Date: 10/18/2018 12:01:00 AM
Voting End Date: 10/22/2018 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 237
Total Ballot Pool: 300
Quorum: 79
Weighted Segment Value: 23.2

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	84	1	12	0.25	36	0.75	16	20
Segment: 2	7	0.4	0	0	4	0.4	2	1
Segment: 3	70	1	5	0.116	38	0.884	12	15
Segment: 4	13	1	4	0.364	7	0.636	1	1
Segment: 5	68	1	13	0.31	29	0.69	10	16
Segment: 6	48	1	7	0.241	22	0.759	11	8
Segment: 7	1	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	0	0	1	0.1	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	8	0.3	1	0.1	2	0.2	3	2
Totals:	300	5.8	42	1.381	139	4.419	56	63

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		None	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Brandon McCormick	Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Abstain	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Corn Belt Power Cooperative	larry brusseau		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Laura Lee		None	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Abstain	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson		Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		None	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	William Sanders		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	Manitoba Hydro	Mike Smith		Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	None	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		None	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Nathaniel Clague		None	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz	Dennis Chastain	Abstain	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Douglas Webb	Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Leanna Lamatrice		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Vo	Gary Nolan	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Exelon	John Bee		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Brandon McCormick	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Negative	Comments Submitted
3	Intermountain REA	David Maier		Negative	Comments Submitted
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	None	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	Brandon McCormick	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	Aaron Smith		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Dan Zollner		None	N/A
3	PPL - Louisville Gas and Electric Co.	Joseph Bencomo		None	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
3	Rutherford EMC	Tom Haire		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		None	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		Negative	Comments Submitted
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	None	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Negative	Comments Submitted
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Douglas Webb	Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Negative	Comments Submitted
4	LaGen	Richard Comeaux		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Negative	Comments Submitted
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Michael Brytowski	Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		None	N/A
5	JEA	John Babik		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	None	N/A
5	NaturEner USA, LLC	Eric Smith		None	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Brett Jacobs		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Affirmative	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Vistra Energy	Dan Roethemeyer		Abstain	N/A
5	Westar Energy	Derek Brown	Douglas Webb	Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Nicholas Kirby		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Abstain	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres		None	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Kris Butler		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Modesto Irrigation District	James McFall	Courtney Lowe	None	N/A
6	Muscatine Power and Water	Ryan Streck		None	N/A
6	New York Power Authority	Thomas Savin	Shelly Dineen	Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Portland General Electric Co.	Daniel Mason		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Comments Submitted
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Westar Energy	Grant Wilkerson	Douglas Webb	Negative	Comments Submitted
6	Western Area Power Administration	Charles Faust		None	N/A
7	Luminant Mining Company LLC	Brenda Hampton		Abstain	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Comments Submitted
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 300 of 300 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Formal Comment Period Open through October 22, 2018
Ballot Pools Forming through October 17, 2018

Now Available

A 20-day formal comment period for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** is open through **8 p.m. Eastern, Monday, October 22, 2018.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues using the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Wednesday, October 17, 2018.** Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

A 5-day initial ballot for the standard, and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **October 18-22, 2018**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | CIP-008-6
Comment Period Start Date:	10/3/2018
Comment Period End Date:	10/22/2018
Associated Ballots:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 IN 1 ST

There were 86 sets of responses, including comments from approximately 176 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The Standard Drafting Team (SDT) created a new definition and modified existing definitions to address the directive in FERC Order No. 848 paragraph 31 regarding "attempts to compromise" without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use existing *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary) definitions. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident, and the proposed new definition of, Reportable Attempted Cyber Security Incident? If not, please provide comments and alternate language, if possible.

2. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? If not, please provide comments and an alternate approach to addressing the directive, if possible.

3. Do you agree with reporting timeframes included Requirement R4? If you disagree please explain and provide alternative language and rationale for how it meets the directives in FERC Order No. 848.

4. The SDT created Attachment 1 to be used for consistent reporting and intentionally aligned the content with FERC Order No. 848 paragraphs 69 and 73. Do you agree with the content and use of Attachment 1?

5. Do you agree with the required methods of notification proposed by the SDT in Requirement R4, Part 4.2? If no, please explain and provide comments.

6. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R4? If no, please explain and provide comments.

7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

8. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

9. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Luminant Mining Company LLC	Brenda Hampton	7		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant	5	Texas RE

						Generation Company LLC		
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Exelon	Chris Scanlon	1		Exelon Utilities	Chris Scanlon	BGE, ComEd, PECO TO's	1	RF
					John Bee	BGE, ComEd, PECO LSE's	3	RF
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Seattle City Light	Ginette Lacasse	1,3,4,5	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC

					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aubrey Short	FirstEnergy - FirstEnergy Corporation	4	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO	SPP CIP-008	Matt Harward	Southwest Power Pool (RTO)	2	MRO
					Louis Guidry	Cleco	1,3,5,6	SERC
Manitoba Hydro	Mike Smith	1		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Associated Electric Cooperative, Inc.	Todd Bennett	1,3,5,6		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The Standard Drafting Team (SDT) created a new definition and modified existing definitions to address the directive in FERC Order No. 848 paragraph 31 regarding "attempts to compromise" without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use existing *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary) definitions. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident, and the proposed new definition of, Reportable Attempted Cyber Security Incident? If not, please provide comments and alternate language, if possible.

Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	

Comment

Does not limit what must be reported, but Entity will need to devote significant resources, which takes away time from addressing cyber attacks

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

PPL NERC Registered Affiliates generally agree with the changes. However, neither the modified term "Reportable Cyber Security Incident" nor the new term "Attempted Cyber Security Incident" appears to include compromise or disruptions of a Cyber Asset supporting a PACS. Specifically, EACMS and ESP are mentioned, but a PSP is not.

This omission of Cyber Assets supporting a PACS, if purposeful, seems inconsistent with other NERC guidance. We would suggest either providing clear rationale for this omission or correcting the language for consistency if it was not left out on purpose.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	Revisions to Defined Terms.docx

Comment

AZPS recommends that the proposed definitions be reviewed to ensure there is not redundancy of terms within other defined terms as such redundancy can result in unintended consequences. For example, the term Cyber Security Incident references attempts to compromise. Thus, the incorporation of the same or similar verbiage into the newly proposed term Reportable Attempted Cyber Security Incident is not necessary. Accordingly, APS proposes the revisions to the defined terms Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident shown in the attached.

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

American Transmission Company LLC (ATC) supports the proposed new and modified definitions; however, believes there may be opportunity for further improvement. ATC offers the following perspective and rationale and requests the SDT consider this as an alternative approach:

The existence of the Physical Security Perimeters (PSPs) within the Cyber Security Incident definition causes confusion within the Requirements. To gain ultimate clarity, ATC requests the SDT remove PSP from the Cyber Security Incident definition and consider the creation of a second new definition to assure Registered Entity's Cyber Security Incident Planning and Response Programs continue to take into account a Cyber Security breach that may occur through physical means. ATC offers the proposed draft definition language as originally directed by FERC in Order 706 paragraph 656:

Potential Cyber Security Incident (new definition):

A malicious physical act or suspicious physical event that:

- Compromises, or was an attempt to compromise the Physical Security Perimeter or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Cyber Security Incident (adjustments to proposed modified definition):

A malicious act or suspicious event that:

- Has been determined to be a Potential Cyber Security Incident
- Compromises, or was an attempt to compromise the Electronic Security Perimeter or Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

ATC asserts this approach:

1. May help simplify and clarify the scope of the Definitions, Requirement language, and Attachment 1,

2. Remove the ambiguity that a physical act/event alone constitutes a cyber act/event; thereby removing the opportunity for interpretative debate of what could be 'perceived' or 'implied' as reportable under CIP-008. This helps clarify that physical acts/events involving a PSP are to be treated as cyber 'potentialities'.

3. Draws a clearer tie between CIP-006 and CIP-008 while adding clarity to the relationship between physical acts/events that may manifest into cyber acts/events,

4. Retains the obligation for Registered Entities to investigate physical acts/events as potential attack vectors for Cyber Security Incidents that, once determined, must trigger Cyber Security Incident Response,

5. Achieves the current and historical FERC directives, and

6. Does not change the intention nor results of Cyber Security Incident planning and response.

Next, to complete this concept, the Requirement language could be modified as follows:

A. Add 'BES" in front of "Cyber Security Incident Response plan(s)" in CIP-008-6 Requirement R1 to draw a clear tie to CIP-006-6 Requirement R1 Parts 1.5, 1.7, and 1.10 without having to open CIP-006 for modifications. Proposal:

R1. Each Responsible Entity shall document one or more BES 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].*

B. Add the explicit obligation to investigate Potential Cyber Security Incidents to Requirement R1 Part 1.1. Proposal:

One or more processes to:

1. Investigate Potential Cyber Security Incidents, and

2. Identify, classify, and respond to Cyber Security Incidents.

C. Remove the confusing PSP exclusion from Requirement R4 Part 4.1. Proposal:

Initial notifications and updates for Reportable Cyber Security Incidents and/or Reportable Attempted Cyber Security Incidents shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;
2. The attack vector used; and
3. The level of intrusion that was achieved or attempted.

D. Simplify CIP-008-6 Attachment 2, by removing the 'Note' about PSP(s) from Section: Incident Type, Field Name: Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Under # 3 in the proposed modification of terms, The term Electronic Access control of monitoring should read Electronic Access control or monitoring systems. We think the definition to be overly broad, determining what is an “attempt” or “suspicious” is not defined entities will not apply the definition consistently. The SDT should consider including PACS. Should not include physical security perimeter because it is inconsistent with the definition to only include cyber incidents.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Propose adding ‘as determined by the entity’ to the definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

WECC voted yes to approve the revisions to CIP-008 but is providing comments for consideration that WECC believes would improve the Standard.

The “Cyber Security Incident” Definition needs to be revised to, "*[…] (3) Electronic Access Control **OR** Monitoring System for High or Medium Impact BES Cyber Systems, […]"* rather than "*Control OF Monitoring."*

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

NRG requests that NERC consider providing additional clarity in definition of Reportable Cyber Security Incident to further specify "attempt" meaning in the "Reportable Attempted" term (for example, intentional attempt) within the glossary of terms (NERC) or within the technical guidance of the draft standard changes relating to CIP-008-6.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment
AECI supports the comments provided by NRECA.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment
The proposed revised definitions of Reportable Attempted Cyber Security Incident and Reportable Cyber Security incident appear to expand on the definition of EACMS. The both include the following language: "*Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting*." Texas RE recommends that it would be cleaner to include these functions in the definition of EACMS. In the proposed definition of Reportable Attempted Cyber Security Incident, the phrase "*attempt to compromise or disrupt*" is very broad. Texas RE recommends describing in detail what this means. Texas RE is concerned the proposed language may allow for entities not reporting threats to Physical Security Perimeters (PSP). First, the proposed definition of Cyber Security Incident includes the PSP. The proposed definition of Reportable Cyber Security Incident does not include PSP. Additionally, Part 4.1 includes the language, "*Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter*". A compromised Physical Security Perimeter could be just as damaging as a compromised Electronic Security Perimeter. Texas RE recommends the definition of Reportable Cyber Security Incident and Part 4.1 apply to PSPs as well.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	
Document Name	

Comment

Luminant does not agree with the proposed definition for Reportable Attempted Cyber Security Incident. As currently written there are no boundaries on what constitutes an “attempt” which will lead to different interpretations and therefore inconsistent enforcement. For example, would malware present on a Transient Cyber Asset that is detected during a scan of that asset be considered an attempt to compromise or disrupt reliability tasks, an ESP or EACMS? At its very core, all malware is an attempt to compromise something, but the majority of malware is not at all targeted toward disrupting power operations. Another example is extensive scanning to identify weaknesses and gather any available information. While this is often the first step of an actual attack, it is also often not targeted or performed by inexperienced actors. While such activities should be noted and investigated, in and of themselves they are generally not treated as actual or attempted cyber security incidents.

Luminant recommends the SDT clarify the intent of this reporting. If the focus is to establish a more extensive baseline understanding of the nature of cyber security threats and vulnerabilities encountered within the industry than perhaps we can create a treatment similar to aggregate self-logging for “minimum risk” events that require periodic reporting. The examples above would be included in such reporting. This approach could reduce the debate over what constitutes an “attempt” and an entity can be considered in compliance as long as the event is reported. Much like aggregate self-logging, if the ERO disagrees that an activity is “minimum risk,” they can address that individually and disseminate lessons learned to evolve the definition. In this approach, an event that has clear indicators of intent to disrupt reliability tasks, ESPs, PSPs, EACMS or BCS would not be eligible for aggregate reporting and would instead follow a more rigorous approach.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

APPA appreciates the drafting team working to address FERC’s directives while preserving the integrity CIP-003’s scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below.

APPA’s concern with the proposed definition is due to the use of, “one or more reliability tasks of a functional entity.” The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks.
For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern:

Reportable Attempted Cyber Security Incident:
A Cyber Security Incident that was an attempt to compromise or disrupt:
• the operation of a BES Cyber System; or
• Electronic Security Perimeter; or
• Electronic Access Control or Monitoring System (EACMS) that provide any of the

following functions: (1) authentication; (2) monitoring and logging; (3) access control;
(4) Interactive Remote Access; or (5) alerting.

Additionally, the phrase “attempt to compromise or disrupt” introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT has joined the comments of the ISO/RTO Council and offers these supplemental comments.

Regarding the “Cyber Security Incident” definition, “High or Medium Impact BES Cyber Systems” is not necessary in the definition. EACMSs are already limited to High and Medium Impact BES Cyber Systems. Also, the applicability is addressed in the Applicable Systems column of the table with each requirement.

Regarding the definition of “Reportable Cyber Security Incident,” the details of the EACMS functions are not necessary; including the list of functions may have the unintended consequence of excluding things that should be included.

Regarding the definition of “Reportable Attempted Cyber Security Incident,” ERCOT questions the need for this definition. The reporting timelines can be addressed with the requirement parts for compromise vs. attempt to compromise.

Regarding the concept of “attempt”generally, ERCOT requests more specificity and clarification on the types and thresholds of attempts that are expected to be reported. As FERC Order 848 recognized, specificity in the reporting threshold is needed “to ensure that [the reporting obligation] would provide meaningful data without overburdening entities.” FERC Order 848 at ¶ 52 (quoting NERC comments). Lack of specificity will result in differing

interpretations of “attempt” across the industry. A conservative reading of this term could yield substantial over-reporting of activities that do not bear any indication of malicious intent or harm. This could lead to over-reporting of incidents to E-ISAC and ICS-CERT, thereby reducing visibility of reports of legitimate incidents. Other entities may interpret the term in such a way that leads to information regarding important events not being reported. To avoid these results, ERCOT strongly encourages the SDT to identify specific reporting thresholds such as those proposed by the ISO/RTO Council.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The phrase “attempts to compromise” is overly broad. The intent of the scope of this clause should to be more clearly defined as the undefined term could be interpreted in many different ways . Additionally, while we agree with the five criteria proposed, additional criteria for the reporting of an attempted compromise should also be included to address the bounds of attempts.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

How do we measure an attemps to compromise?

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Definitions should not include EACMs. Every packet denied by a firewall would generate a potential Reportable Attempted Cyber Security Incident, making this requirement onerous for the entities.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The definition of “Reportable Attempted Cyber Security Incident” is still unclear. What does it mean to attempt? What includes an attempt?

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Reportable Attempted Cyber Security Incident and Cyber Security Incident have defined inconsistencies such as one references BES operation and the other for Reliability tasks. Reportable Attempted Cyber Security Incident uses "attempt" in the definition and never defines what is an "attempt".	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Security Incident should be expanded to include the desired elements of the proposed new term.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Security Incident should be expanded to include the desired elements of the proposed new term.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	

Comment
Platte River is okay with the draft requirement language as proposed in CIP-008-6. Platte River is recommending a modification be made to the proposed new term: Reportable Attempted Cyber Security Incident. The proposed term assumes the Responsible Entity can determine the intent of the individual whose activity was identified. Since, by definition, the attempt was unsuccessful, the Registered Entity cannot know what the individual was trying to accomplish. The method to implement the definition, as proposed, is not clear. Platte River is recommending the following modifications be made to the definition: Reportable Attempted Cyber Security Incident: A Cyber Security Incident that was an attempt to circumvent: · Electronic Security Perimeter; or · Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting Platte River believes this definition better captures the intent of the changes in CIP-008-6. Registered Entity staff are better able to determine if the individual was attempting to circumvent their security controls without having to determine the individual's intent.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	

Comment
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Securtiy Incident shoudl be expanded to include the desired elements of the proposed new term.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	
Comment	

The proposed definition of “Reportable Attempted Cyber Security Incident” does not provide enough specificity to make a determination as to whether an incident was attempted. Lack of clarity in this definition would make the difference between TVA reporting: 1) only those incidents that had a high potential of success but were not successful; and 2) any and all efforts to gain intelligence about NERC CIP scoped systems. The subsequent reporting of the latter could be overwhelming to TVA, E-ISAC, and ICS-CERT.

In addition, lack of specificity in the definition of the word “disrupt” could have a similar effect. This term should be limited to disruptions from cyber events to avoid reporting of purposeful disruptions (e.g., asset reboots for maintenance purposes). Without this, all maintenance disruptions could be reportable.

Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	
Comment	

The Cyber Security Incident definition is rooted in the law (Section 215) definition: “The term ‘cybersecurity incident’ means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.” This definition clearly identifies the target of the event to be “programmable electronic devices and communication networks.” The current NERC glossary term includes PSPs as a target. PSPs are not “programmable electronic devices and communication networks.” The definition would be better aligned with the law by deleting “Physical Security Perimeter’ from the Cyber Security Incident definition. “Programmable electronic devices and communication networks” create the concept of ESPs or are EACMS. So references in the definition to ESPs and EACMS don’t contradict the law (Section 215).

With the addition of Reportable Attempted Cyber Security Incident, the existing term Reportable Cyber Security Incident should be revised to more clearly delineate the difference between the two terms. For example: Reportable Successful Cyber Security Incident or Reportable Actual Cyber Security Incident. We recognize this would require minor changes in CIP-003. In the webinar, there was also mention of tracking historical metrics with future metrics. It shouldn’t be difficult to add historical metrics to the future metrics especially given there were so few historical metrics. These two items are worth it to minimize confusion.

Likes 0	
Dislikes 0	
Response	

larry brusseau - Corn Belt Power Cooperative - 1

Answer	No

Document Name	

Comment

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

{C}· Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

{C}· Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA appreciates the challenge facing the SDT in addressing the directive regarding "attempts to compromise" as required by FERC Order No. 848. BPA recommends the SDT revise CIP-008-6 to include clear language allowing the entity to define "an attempt." This will take into consideration entities of varying size facing differing threat vectors.

Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The Reportable Attempted Cyber Security Incident definition as written and interpreted by the SDT is intended to provide entities flexibility to define “attempt” and a process around reporting. This may result in a very low threshold that is defined by entities and result in underreporting with no added value. On the flip side, this can also result in unnecessary overload if reporting criteria is set too high. Another concern is that this flexibility also allows for an auditor’s own interpretation of “attempt”. BC Hydro does not see any value-add in making reportable attempts a mandatory requirement as opposed to having this be a voluntary process.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No
Document Name	
Comment	
Physical Security Perimeter (PSP) should be removed from the Cyber Security Incident definition. It is not consistent with the proposed revised Reportable Cyber Security Incident and the proposed new term Reportable Attempted Cyber Security Incident. If the intent is to keep PSP then this should be represented in a new PSP specific definition.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

WEC Energy Group agrees that the new and modified definitions meet FERC's directive in Oder No. 848 and we generally support these definitions except for one term. WEC Energy Group is concerned that the term "attempt to compromise" is ambiguous and insufficiently understood.

The Commission used the term "attempt to compromise" in Order 848 but also stated that the directive was "to augment the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm reliable operation of the BES." (see P2) We believe this was meant to focus the reporting on incidents that represent a clear threat to the BES.

We believe the SDT should consider either defining the term or developing boundaries that can be consistently applied by the industry to provide clearer focus on incidents that have been identified as genuine threats to protected BES Cyber Systems. This would better ensure the term is understood broadly by industry allowing entities to develop measured and consistent processes that ensure new requirements do not interfere or otherwise complicate industry efforts to identify issues that represent serious risks to BES Reliability.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Given that the definition of Cyber Security Incident includes “compromise or was an attempt to compromise”, the definitions of the modified Reportable Cyber Security Incident and the new Reportable Attempted Cyber Security Incident are broad enough to bring almost each Cyber Security Incident to become a reportable one. We disagree that each compromise or was an attempt to compromise of ESP or EACMS needs to be reported unless it affects reliability, in that it may result in millions of reports per year. If it is intended to include attempts of compromise affecting reliability to be reportable, we suggest only to revise the existing Reportable Cyber Security Incident definition rather than creating additional reportable one: “Reportable Cyber Security Incident: A Cyber Security Incident that has compromised or disrupted or was an attempt to compromise or disrupt one or more reliability tasks of a functional entity.”

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

As drafted, it is difficult to discern a difference between the definitions for *Reportable Cyber Security Incident* and *Reportable Attempted Cyber Security Incident*. Additionally, we do not think it is reasonable or necessary to report all "knocks on the door" to our ESPs or EACMS. We propose the following modifications (or something similar) to both defitions so that there is a more clear distinction between the two and clear reporting expectations.

Reportable Cyber Security Incident:

A Cyber Security Incident that has disrupted

- One or more reliability task of a functional entity; or
- BES Cyber System; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Reportable Attempted Cyber Secuirty Incident:

A Cyber Security Incident where there was access into an ESP, or an EACMS, but there was no resulting disruption to the EACMS, BES Cyber System, or a reliability task.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL believes that by modifying the definition of Cyber Security Incident, the intent of the FERC order can be met. The definition of Reportable Attempted Cyber Security Incident is not necessary if these changes are made.

Likes 0	
Dislikes 0	

Response

Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy

Answer	No
Document Name	

Comment

The definition of Reportable Attempted Cyber Security Incident is circular with Cyber Security Incident. The term *Cyber Security Incident* already included the term “attempt” in a different meaning.

Suggested updated definitions:

Cyber Security Incident:

A malicious or suspicious event related to:

- an Electronic Security Perimeter or
- a Physical Security Perimeter or
- Electronic Access Control or Monitoring System for High and Medium Impact BES Cyber Systems

Reportable Cyber Security Incident:

A Cyber Security Incident that successfully compromised or disrupted:

- one or more reliability tasks of a functional entity or
- an Electronic Security Perimeter or
- an Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that attempted to compromise or disrupt:

- one or more reliability tasks of a functional entity or
- an Electronic Security Perimeter or
- an Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Attempted should also be defined to provide the appropriate guidance as to what constitutes a Reportable Attemped Cyber Security Incident. Some possible items to include as an attempt are:

- was directed specifically at or appeared to be specifically directed at an ESP, ECASM or BCA
- was not incidental to other network activity, including bulk, non-specific undesired network activity

could have feasibly compromised an ESP, EACMS or BCA by its very nature

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

• Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

• Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

ALSO:

Reclamation recommends the definition for Reportable Attempted Cyber Security Incident be expanded to include disruption or attempted compromise of Physical Security Perimeters and Physical Access Control Systems. This would allow identifying a Facility as a potential target without its reliability or operations being affected.

Reclamation also recommends removing the following language from the bullet point for EACMS because it is redundant of the EACMS definition: *"that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

Therefore, Reclamation recommends the proposed new term be changed

from:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

One or more reliability tasks of a functional entity; or

Electronic Security Perimeter; or

Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

to:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

One or more reliability tasks of a functional entity; or

Electronic Security Perimeter (ESP); or

Physical Security Perimeter, including locally-mounted hardware or devices; or

Physical Access Control Systems (PACS); or

Electronic Access Control or Monitoring System (EACMS).

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	No
Document Name	

Comment

"attempted" is to broad of a term. Our SMEs have concerns that the term could be viewed to broadly which could then in turn result in altert fatique and credible indicents could then be missed.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

The phrase ". . . an attempt to . . ." in the proposed modification of the term Cyber Security Incident and in the proposed new term Reportable Cyber Security Incident is too vague. Modification of the phrase ". . . an attempt to . . ." to ". . . an attempt, which, if successful, would have resulted in the compromise or disruption . . ." or something similar seems to be closer to the intent of the proposed changes.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

Due to a lack of published draft Implementation Guidance, it is challenging to fully assess the impacts of the new “Reportable Attempted Cyber Security Incident” definition and the addition of EACMS in terms of how much additional investigation and reporting volume will fall on the Responsible Entity. Providing specific guidance with examples of what would and would not be a “Reportable Attempted Cyber Security Incident” may alleviate these concerns.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Agree with the language of the definition, but believe that the addition of a new definition so closely related and worded to two existing definitions could cause confusion among industry. Would suggest revisiting the topic as a SDT.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, NRECA believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team’s approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. NRECA urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agrees with APPA's comments. Additionally, we note that the definition of Reportable Attempted Cyber Security Incident (as well as that of Reportable Cyber Security Incident) not including a Cyber Security Incident to a Physical Security Perimeter that does not compromise or disrupt one of the three bulleted items, and wonder if that was an intentional decision.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We are concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, we believe that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. We urge the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	
Comment	

- Overall our SMEs believe this standard should focus more on the risk and benefits of monitoring events within the power grid versus work, effort and expense of collecting data on potential cyber intrusions.Second bullet fails to capture the "… for High or Medium Impact BES Cyber Systems…"Proposed Modified Term, "Reportable Cyber Security Incident" - None of the listed bullets currently capture Physical attacks or compromises of the physical perimeter.Recommend deleting the term "Reportable Attempted Cyber Security Incident" and modifying the definition of Reportable Cyber Security Incident to include the following: A Cyber Security Incident that has compromised, disrupted or was an attempt to compromise or disrupt
- Also agree with NPCC submitted comments

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

I support all comments submitted by Terry Harbour, Berkshire Hathaway Energy-MidAmerican Energy Company.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Definitions do not limit what must be reported. Entity will need to devote significant resources to reporting – which takes away resources from addressing cyber attacks

Some concern with "Reportable Cyber Security Incident" for field locations (substations & generators) since these locations have fewer defense layers.

Concerns that the "Cyber Security Incident" puts the burden of determining intent – is the intent to "compromise" or "disrupt." Expect this lack of clarity to result in in over-reporting which makes finding the real incident akin to a needle in the haystack.

Likes 0	
Dislikes 0	

Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	
Comment	
GSOC is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, GSOC believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. GSOC urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

Proposed modified terms and Proposed new term include a separate definition for EACMS when compared to the current EACMS definition in the NERC Glossary. The proposed modifications and proposed new term should reference the existing definition of EACMS. There should be no difference in identifying EACMS for incident reporting purposes vs systems already identified as EACMS.

Proposed modified terms and Proposed new term include the phrases “attempt to compromise” and “attempt to disrupt”. Further clarification is needed for the meaning of these phrases to guide Responsible Entities on reporting requirements.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

Vectren agrees with the modified definitions of Cyber Security Incident and Reportable Cyber Security Incident. However, the new definition of Reportable Attempted Cyber Security Incident is very broad which leaves it open to interpretation. This definition as written will cause an unreasonable administrative burden on the entity, requiring us to dedicate significant time and resources to track and investigate potential attempts.

By investigating blocked attempts, the focus is shifted away from higher risks. The resources of E-ISAC and ICS-CERT will also be impacted by a larger volume of reports regarding lower risk threats including the potential attempts to compromise. Ultimately, this shift in focus could lead to a compromise of safety and reliability of the BES.

Recognizing the task of the SDT to draft a reasonable definition, the definition in its present form will not serve the intent of the FERC Order No. 848 directive. We would suggest the SDT narrow the scope of “attempts to compromise” within the definition to alleviate the potential burden to the entity, E-ISAC and ICS-CERT.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The proposed modification to the definition of Reportable Cyber Security Incident indirectly alters and expands the current definition of Electronic Access Control or Monitoring System (EACMS), potentially bringing into scope Cyber Assets for CIP-008 reporting that Responsible Entities had not previously determined in scope for CIP overall. CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) proposes that the language following

the listing of EACMS in the Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident definitions, "*that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting"* be removed.

For the proposed new term of Reportable Attempted Cyber Security Incident, the determination of intent in the phrase "attempt to compromise or disrupt" is subjective and therefore difficult to apply as a standard. Any packet or connection rejected by a firewall, access control list, or logged access attempt could be interpreted as existing security controls working as designed or as an attempted compromise to possibly report. This could be millions of attempts, per day, per EACMS under normal operations. No Technical Rationale or Implementation Guidance is offered to assist with characterization of an attempt to compromise or compromise of an EACMS. CenterPoint Energy acknowledges the Technical Rationale and Justification provided by the SDT and the ongoing efforts to update the Guidelines and Technical Basis of the CIP Standards. For the benefit of these modifications, successful ballot, and implementation, CenterPoint Energy suggests that the SDT coordinate with the CIP Guidelines and Technical Basis Review team to provide the revised guidance with this project's materials or adjust the Implementation Plan to allow for the development of the guidance well in advance of the effective date. Most notably, the guidance should assist with characterization of an attempt to compromise or compromise of an EACMS.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends that further clarification be given on what constitutes an actual "attempt" when determining whether a Reportable Attempted Cyber Security Incident has occurred. Perhaps this could be made clearer in an Implementation Guide with examples of what an "attempt" should be considered as.

Likes 1	Long Island Power Authority, 1, Ganley Robert
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	No
Document Name	

Comment

More guidance is needed regarding the definition of what constitutes an "attempt."

Likes 0	
Dislikes 0	

Response
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with the below comments from APPA: : APPA appreciates the drafting team working to address FERC's directives while preserving the integrity CIP-003's scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below. APPA's concern with the proposed definition is due to the use of, "one or more reliability tasks of a functional entity." The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks. For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern: **Reportable Attempted Cyber Security Incident:** A Cyber Security Incident that was an attempt to compromise or disrupt: · the operation of a BES Cyber System; or · Electronic Security Perimeter; or · Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting. Additionally, the phrase "attempt to compromise or disrupt" introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?

Likes 0	
Dislikes 0	

Response
Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	
Comment	

Attempts to compromise are a constant in an interconnected world. Expanding the criteria of Reportable Incidents will be burdensome to entities and NERC without considerable benefit. The CIP standards and the protections required within are what reduce cybersecurity risk and prevent attempts to compromise. Any unsuccessful attempts are a sign the controls are working and are not incidents, they are cybersecurity events. Where controls fail or are bypassed and or compromised ie an actual incident[1], should be the only Reportable Cybersecurity Incident.

{C}[1]

Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	
Comment	

The proposed new term ""Reportable Attempted Cyber Security Incident"" is redundant. Already included within the definition of "Cyber Security Incident" is the statement *"or was an attempt to compromise"*. Therefore the defined term of a "Reportable Cyber Security Incident" is inclusive of this condition. A solution would be to indicate the nature of the reportable event as successful, or attempted.

In addition, ITC concurs with the follwing comments submitted by SPP:

"**Grammatical Issues:** The draft definition for Cyber Security Incident contains a typographical error that should be fixed prior to final ballot. The terms should be "Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems."

Additionally, the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident should reference EACMS consistent with the general definition of Cyber Security Incident: "Electronic Access to Control or Monitoring System (EACMS) for High or Medium Impact BES Cyber Systems that provide the following functions…"

Substantive Issues: The proposed definitions of "Cyber Security Incident" and "Reportable Attempted Cyber Security Incident" includes the language "attempt to compromise or disrupt" as an element of the condition. The statement "attempt to compromise or disrupt" is unclear, ambiguous, and should be further defined by criteria. The SSRG supports the following categories proposed by the SWG in its comments:

- If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.
- Insider incidents involving access to ESP's.
- Incidents involving ICS systems (such as ICCP network or server equipment).

- Incidents involving Physical access that could involve BES Cyber Systems.
- Events and incidents noted as involving ESP's.
- Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). "

Does this need to address entity definition of attempt (confirmed attempt?). Does the exclusion of PSP attempts and disruption make sense as far as reporting goes? PSP's would seem to be as important as ESP's in this regard.

With regard to the proposed definition of "Reportable Cyber Security Incident": Should this simply be EACMS without restriction or one of other descriptions of EACMS?

With regard to the proposed definition of "Reportable Attempted Cyber Security Incident": Is this definition needed given the prior definitions (note "attempt" shows up in Cyber Security Incident already)?"

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI agrees that the new and modified definitions meet FERC's directive in Oder No. 848 and we generally support these definitions except for one term. EEI is concerned that the term "attempt to compromise" is ambiguous and insufficiently understood.

The Commission used the term "attempt to compromise" in Order 848 but also stated that the directive was "to augment the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm reliable operation of the BES." (see P2) We believe this was meant to focus the reporting on incidents that represent a clear threat to the BES.

We believe the SDT should consider either defining the term or developing boundaries that can be consistently applied by the industry to provide clearer focus on incidents that have been identified as genuine threats to protected BES Cyber Systems. This would better ensure the term is understood broadly by industry allowing entities to develop measured and consistent processes that ensure new requirements do not interfere or otherwise complicate industry efforts to identify issues that represent serious risks to BES Reliability.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
With the addition of Reportable Attempted Cyber Security Incident, the existing term Reportable Cyber Security Incident should be revised to more clearly delineate the difference between the two terms. Actual and attempted compromise of assets including EACMS. The word “attempt’ can be defined differently than what the OE-417. An “attempt” could be reportable if a declared incident could potentially affect our in-scope assets. Each entity has a threshold that depends on the resources and skills that they have. EACMs have attempts every day. We could not find language defining an “attempt to compromise”. The current NERC glossary term includes PSPs as a target. PSPs are not, “programmable electronic devices and communication networks.” The definition would be better aligned with the law by deleting, “Physical Security Perimeter” from the Cyber Security Incident definition. “Programmable electronic devices and communication networks” create the concept of ESPs or are EACMS. So references in the definition to ESPs and EACMS don’t contradict the law (Section 215	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Proposed modified terms and Proposed new term include a separate definition for EACMS when compared to the current EACMS definition in the NERC Glossary. The proposed modifications and proposed new term should reference the existing definition of EACMS. There should be no difference in identifying EACMS for incident reporting purposes vs systems already identified as EACMS.	

Proposed modified terms and Proposed new term include the phrases “attempt to compromise” and “attempt to disrupt”. Further clarification is needed for the meaning of these phrases to guide Responsible Entities on reporting requirements.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
What constitutes an attempt? Without a clearer definition, the concern is that we will be reporting attempts every day and having continuous follow-up reporting for things that may not necessarily add any additional security. The Standard should provide criteria for attempts and/or make it clear within the requirement that the Entity defines a process to make that determination. If not, it is left open for auditor interpretation and potential violations for not reporting something they think should have been reported.	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	
Tacoma Power agrees with APPA's comments: "APPA appreciates the drafting team working to address FERC’s directives while preserving the integrity CIP-003’s scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below. APPA’s concern with the proposed definition is due to the use of, “one or more reliability tasks of a functional entity.” The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks. For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern: **Reportable Attempted Cyber Security Incident:**	

A Cyber Security Incident that was an attempt to compromise or disrupt:
· the operation of a BES Cyber System; or
· Electronic Security Perimeter; or
· Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Additionally, the phrase “attempt to compromise or disrupt” introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?"

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper believes that “Attempted” in Reportable Attempted Cyber Security Incident needs to be defined further. The SDT should provide guidance on what needs to be reported as a Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The phrase “for High or Medium Impact BES Cyber Systems” should be removed from the definition for Cyber Security Incident. Applicability information should be in the Standards and requirement language, not in definitions. Although Low Impact facilities are not required to define an ESP or EACMS, entities that have defined these controls at Low Impact assets should report compromises or attempted compromises to the ESP or EACMS if they detect them.

Likes 0	
Dislikes 0	

Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

Comments: APPA appreciates the drafting team working to address FERC's directives while preserving the integrity CIP-003's scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below.

APPA's concern with the proposed definition is due to the use of, "one or more reliability tasks of a functional entity." The proposed definition of Reportable Attempted Cyber Security Incident and that term, introduce ambiguity in determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks.

For example in the event of a ransomware attack that affected an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or was the attacker's intent financial gain? The following definition attempts to eliminate this concern:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:
· the operation of a BES Cyber System; or
· Electronic Security Perimeter; or
· Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

We agree with EEI's comments for this question.

Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments. The term “attempts to compromise” could be construed as vague because it does not clearly define what constitutes a reportable attempt, which could create an undue reporting burden on entities without a commensurate reliability benefit. Many entities receive thousands of attempts to comprise their networks daily, and most have nothing to do with the EMS system. The standard should make clear that “attempts” of that kind should not be reportable.	
Likes 0	
Dislikes 0	

Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Currently, NERC does not define what an “Attempt” is. An “attempt” could vary from entity to entity depending on how an individual defines the term. The language “attempt” could be comprised of anything; the wording of a “Cyber Security Incidents that compromise, or “attempt” to compromise, a responsible entity’s ESP or associated EACM…”is vague and ambiguous. Not only does “attempt” needs to be defined so does “detected. If one perceives there to be an “attempt” what are the measures/definition for “detecting” the “attempt.”	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	No
Document Name	
Comment	
Definitions do not limit what must be reported. Entity will need to devote significant resources to reporting – which takes away resources from addressing cyber attacks	

Some concern with “Reportable Cyber Security Incident” for field locations (substations & generators) since these locations have fewer defense layers.

Concerns that the “Cyber Security Incident” puts the burden of determining intent – is the intent to “compromise” or “disrupt.” Expect this lack of clarity to result in in over-reporting which makes finding the real incident akin to a needle in the haystack.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

David Maier - Intermountain REA - 3

Answer	No
Document Name	

Comment

The issue with this draft is the potential for application inconsistency based on what is assumed to be an “attempt”. Neither “Attempts to compromise” nor “attempt” have been defined by the SDT.

1. attempt” should be properly defined by the SDT to remove ambiguity. In defining what constitutes an attempt, the SDT may require evidence of intent and relate all actions and packets from a campaign as a single attempt report.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

The concerns about expanding the scope of EACMS into CIP-003-6 (or -7) appear to be misplaced. The requirements that are applicable to EACMS are clearly identified in the “Applicable Systems” column in each Requirement table. Even if Low Impact Cyber Assets should meet the definition of EACMS, they would not be subject to those related requirements unless explicitly included in the corresponding “Applicable Systems” column. Mixing applicability of EACMS into a Term definition goes against norms established in the rest of CIP Standards, regardless of whether “High or Medium Impact” is also added. Suggest removing “High or Medium Impact” from the CSI definition.

The concept of Reportable Attempted Cyber Security Incident (RACSI) and the resulting definition of “Reportable Cyber Security Incident” (RCSI) is unnecessarily complicated, counter-intuitive, and results in unnecessarily verbose additions to the requirements. The term “Cyber Security Incident” (CSI) includes both attempted and “successful” cases of being disrupted/compromised. RCSI is confusing because it adds to CSI reporting requirements but subtracts the attempted incidents, with only the former reflected in the name. As such, the name “RCSI” erroneously suggests it

includes all CSI that meet additional reporting requirements. A more complete name might address this concern however this doesn't address the remaining concerns.

The proposed RSCI and RACSI terms separate out attempted and "successful" reportable CSI, which results in having to name both whenever referencing reportable CSI. This results in the need to repetitively insert "Reportable Attempted Cyber Security Incident" after "Reportable Cyber Security Incident" 14 times (including the missed additions in M4 and probably R4.1). The only standalone use of RACSI occurs in R4.3 to specify the different reporting timelines. A more concise and intuitive approach would be to define RCSI only as the CSI that meet the conditions that make it reportable (ie. Not PSP related) and thus include both attempted and "successful" CSI.

This would avoid the need to verbosely replace "RCSI" with "RCSI and/or RACSI" the 14 times. It is suggested that RACSI be abandoned and instead a new term should be adopted that encompasses the RCSI that meet the additional Compromising or Disruptive criteria. Possible names might include variations including "Compromise" or "Disrupt" (C/DRSCI? RC/DSCI?) but seem unwieldy. Incorporating the word "successful" as used above is unhelpful because it is a so called "success" only from the attacker's perspective. We suggest using the term "Reportable Cyber Security Attack" (RCSA), which describes both variations while clearly and concisely indicating it is more serious than a mere RCSI. Other names might be more appropriate, but we will use RSCA for the rest of this comment.

The advantages of using the existing CSI, the redefined RSCI, and the new RSCA terms would be:

· they build on each other intuitively

· a single term exists to express the context mentioned by each (sub-)requirement. (ie. No need to list combinations of CSI, RCSI, or RCSA in the text of any (sub-)requirement)

In addition to the above concerns, the proposed CSI, RCSI, and RACSI definitions use similar but differently worded inclusions that is unnecessarily complicated and may lead to unintended interpretations. For CSI, consider:

· Reference to ESP and EACMS seems redundant as what component of an ESP is not an EACMS? And all EACMS are being included in the "Applicable System" column anyway. EACMS do not need to be mentioned in the definitions.

For RCSI and RACSI, consider:

· By definition, a BES Cyber System (BCS) embodies one or more "reliability tasks" and under CIP-002, all such cyber assets supporting those tasks must be grouped into a BCS. Therefore the "Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System" in CSI is equivalent to "One or more reliability tasks of a functional entity" in RSCI/RACSI. Why should RSCI/RCSA be based on CSI but then restate this?

· Use of the words "compromise" and "disrupt" are inconsistent. CSI applies only "compromise" to the first inclusion and "disrupt" to the second. RSCI/RASCI uses "compromised or disrupted" for all of its inclusions, however it is limited to only the inclusions that exist for CSI, so the RSCI/RASCI inclusions appear broader than they are. For instance, a non-disruptive compromise of a BCS cyber asset would not be included by the proposed RSCI/RASCI definitions because it doesn't meet the CSI inclusions.

· Redefinition of EACMS (functions 1-5) seems entirely redundant and should be removed even though that terminology was used by FERC in its order. Even if EACMS includes some unlisted function other than the 5 mentioned, it would still be included by the fact that all EACMS are being added to the "Applicable Systems" column.

The logical intersection of RCSI or RACSI definition with CSI definition and inclusion of above considerations leaves RCSI/RACSI with effectively only the following much more narrow inclusions:

· Disruption of a BCS

· Compromise of an ESP

The following proposed term definition approach captures the intent of the drafted definitions without the confusing parallel language:

CSI: A malicious act or suspicious event that attempts or succeeds in compromising or disrupting:

· a reliability function of a BES Cyber System

· an ESP

· a PSP

RCSI: A CSI where the compromise or disruption has been confirmed, excluding those incidents that solely involve a PSP.

RACSI: A CSI where the compromise or disruption has not been confirmed, excluding those incidents that solely involve a PSP.

BCS applicability (High, Medium, Low) and related EACMS still identified in the “Applicable Systems” as per convention.

The phrasing also ensures when a CSI involves both the cyber and physical aspects, the CSI is still reportable.

If combined with the earlier suggestion of using alternate terms CSI, RCSI, and RCSA, the definitions could be as follows or similar:

CSI: Same as above approach.

RCSI: A CSI for which the actual or attempted compromise or disruption does not solely involve the PSP.

RCSA: A RCSI for which the compromise or disruption is confirmed to have occurred [rather than merely be attempted]

Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

With regard to the proposed definition of “Cyber Security Incident”, the notion of attempts seems to be left to the responsible entity to define as part of process development. The SWG proposed the following categories of attempts at compromise of the BES for responses to the NOPR (Docket Nos. RM18-2-000 and AD17-9-000) : “…Some criteria for events and incidents that should be reported include:

- If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.
- Insider incidents involving access to ESP’s.
- Incidents involving ICS systems (such as ICCP network or server equipment).
- Incidents involving Physical access that could involve BES Cyber Systems.
- Events and incidents noted as involving ESP’s.
- Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). “

It may be that such lists of criteria for categories of attempts belong in Implementation Guidance more than the standard requirement language itself. The drafting team should include language in either the standard or the guidance to clarify the role of the responsible entity in defining attempts in a manner that lends itself to effective compliance monitoring.

In the definition of Reportable Cyber Security Incident, the SWG proposes that Electronic Access Control or Monitoring System (EACMS) not be limited to specific functions. This will enable clear use of existing categorization of cyber assets without confusion or added burden of sub-categorization for EACMS cases.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	No
Document Name	

Comment

Grammatical Issues: The draft definition for Cyber Security Incident contains a typographical error that should be fixed prior to final ballot. The terms should be “Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems.”

Additionally, the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident should reference EACMS consistent with the general definition of Cyber Security Incident: “Electronic Access to Control or Monitoring System (EACMS) for High or Medium Impact BES Cyber Systems that provide the following functions…”

Substantive Issues: The proposed definitions of “Cyber Security Incident” and “Reportable Attempted Cyber Security Incident” includes the language “attempt to compromise or disrupt” as an element of the condition. The statement “attempt to compromise or disrupt” is unclear, ambiguous, and should be further defined by criteria. The SSRG supports the following categories proposed by the SWG in its comments:

{C}· If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.

{C}· Insider incidents involving access to ESP’s.

{C}· Incidents involving ICS systems (such as ICCP network or server equipment).

{C}· Incidents involving Physical access that could involve BES Cyber Systems.

{C}· Events and incidents noted as involving ESP’s.

{C}· Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). “

Does this need to address entity definition of attempt (confirmed attempt?). Does the exclusion of PSP attempts and disruption make sense as far as reporting goes? PSP’s would seem to be as important as ESP’s in this regard.

With regard to the proposed definition of “Reportable Cyber Security Incident”: Should this simply be EACMS without restriction or one of other descriptions of EACMS?

With regard to the proposed definition of “Reportable Attempted Cyber Security Incident”: Is this definition needed given the prior definitions (note “attempt” shows up in Cyber Security Incident already)?

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	No
Document Name	2018_ 02_ CIP 008 6_ 102218 Final Comments.docx

Comment

Comments: The current draft does not provide clarity on what constitutes an attempt. Attempt is not a defined term and does not identify that the entity may come up with a methodology or approach on what constitutes an attempt. Including attempt “as is” leaves room for differences of opinion on what an attempt is and could be interpreted differently among entities and auditors. Exelon suggests including a requirement for entities to develop a process to define attempts. A defined term may be overly prescriptive, and inhibit the evolution of information sharing. Separately, the standard drafting team should clarify the Cyber Security Response obligations related to PSPs by removing Physical Security Perimeters from Cyber Security Incident definition unless its paired with the breach to an ESP or EACMS. As the proposed Cyber Security Incident definition reads, it could be interpreted that a PSP breach alone constitutes a Cyber Security Incident

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy recognizes and supports the good work that the CIP-008-6 Standards Drafting Team (SDT) has done in addressing the Commission's objectives, identified in Order 848, for modifications to Cyber Security Incident Reporting. While Xcel Energy generally agrees with the SDT's direction, we believe that some further clarification is needed for the proposed definitions for Cyber Security Incidents, Reportable Cyber Security Incidents, and Reportable Attempted Cyber Security Incidents. To remedy the lack of clarity we believe exists around these terms Xcel Energy suggests the following three changes be made:

1. Retirement of the term Cyber Security Incident
2. Modify the term Reportable Cyber Security Incident to read as follows:

Reportable BES Cyber Security Incident:

A malicious act or suspicious cyber event that compromises an Electronic Security Perimeter or Electronic Access Control or Monitoring System (EACMS) of a High or Medium Impact BES Cyber System or; compromises or disrupts the operation of a High or Medium Impact BES Cyber System.

3. Modify the new term Reportable Attempted Cyber Security Incident to read as follows:

Reportable Attempted BES Cyber Security Incident:

A malicious act or suspicious cyber event that was an attempt to compromise an Electronic Security Perimeter (ESP) or Electronic Access Control or Monitoring System (EACMS) of a High or Medium Impact BES Cyber System or; was an attempt to compromise or disrupt the operation of a High or Medium Impact BES Cyber system.

If the SDT opts to keep all three definitions, Xcel Energy would suggest they be changed to read:

BES Cyber Security Incident:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise the Electronic Security Perimeter or Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems; or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system*.

Reportable BES Cyber Security Incident:

A BES Cyber Security Incident that results in an actual compromise or disruption

Reportable Attempted BES Cyber Security Incident:

A BES Cyber Security Incident that was an attempt to compromise or disrupt

The suggested changes above are based on the following issues identified by Xcel Energy:

- Xcel Energy removed the list of EACMS in the above suggested definitions. It is our belief that listing the types of EACMS that apply is redundant. The only EACMS that would have been excluded would have been intermediate systems. However, by including any EACMS that have IRA we have brought intermediate systems back into scope. Also, if the type of EACMS in scope needs to be incorporated, inserting it in these definitions may be problematic. If the distinction needs to be made about the types of EACMS, we suggest it be contained with the Standard itself.
- Xcel Energy is also concerned with the inclusion of "one or more reliability tasks of a functional entity" as it is superfluous and very vague. The use of the term is already contained in scope of CIP-002. The inclusion of the term BES Cyber Systems in the proposed changes to definitions above incorporates the intent of including the "one or more reliability tasks of a functional entity" language. It would be best to remove this wording to avoid any undue confusion that could result.

- The current definition of a Cyber Security Incident includes language for the attempt or compromise of a Physical Security Perimeter (PSP) and the modified definition includes the references to PSPs as well. However, all reporting Requirements and definitions of Reportable Cyber Security Incidents and attempts exclude PSPs. This leads us to inquire what the role of a PSP in a Cyber Security Incident is. Physical Security compromises are already reported under EOP-004 R2 to law enforcement. Responsible Entities could report on compromises to Physical Access Control Systems but those were not included in the FERC Order 848. Xcel Energy would recommend removing references to Physical Security from the proposed modification to the Cyber Security Incident definition. Or the Standard Drafting Team should identify the role the PSPs have in a Cyber Security Event and when they do not need to be reported under the requirements.

- Xcel Energy believes the BES should be added to the definitions for Cyber Security Incidents, Reportable Cyber Security Incidents, and Reportable Attempted Cyber Security Incidents. Xcel Energy notes that a "cyber security incident" is a common term used broadly across many industries and throughout the Xcel Energy enterprise, with the term already existing in many policies, plans, and procedures that do not apply to a BES. NERC's use of the term applying strictly to incidents affecting the BES creates clarity issues in documentation that uses the term more broadly. Xcel Energy uses an enterprise wide cyber security center that monitors, investigates, and responds to all types of cyber security events, regardless of their BES designation. Using common terminology and only applying it to events that affect BES systems will make it more difficult to internally differentiate between those incidents that relate to the BES and those that do not. Adding BES to these terms will allow Responsible Entities to update internal documentation in such a way to avoid confusion events and appropriate responses to those events.
- In the modified term for Cyber Security the new (3) lists "Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;" The "of" should be removed and replaced with "or."

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Need to draw some boundaries around what does (and does not) constitute an attempted compromise. Too burdensome on small entities with no "floor" on what might constitute an attempted compromise.

Likes 0	

Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	

Comment
Vectren agrees with the modified definitions of Cyber Security Incident and Reportable Cyber Security Incident. However, the new definition of Reportable Attempted Cyber Security Incident is very broad which leaves it open to interpretation. This definition as written will cause an unreasonable administrative burden on the entity, requiring us to dedicate significant time and resources to track and investigate potential attempts. By investigating blocked attempts, the focus is shifted away from higher risks. The resources of E-ISAC and ICS-CERT will also be impacted by a larger volume of reports regarding lower risk threats including the potential attempts to compromise. Ultimately, this shift in focus could lead to a compromise of safety and reliability of the BES. Recognizing the task of the SDT to draft a reasonable definition, the definition in its present form will not serve the intent of the FERC Order No. 848 directive. We would suggest the SDT narrow the scope of “attempts to compromise” within the definition to alleviate the potential burden to the entity, E-ISAC and ICS-CERT.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Without additional parameters around the specifics of what constitutes an “Attempt to Compromise”, Southern Company asserts that the requirements are painted with too broad a brush. Further defining “Cyber Security Incident”, “Attempt to Compromise”, “Reportable Attempted Cyber Security Incident”, and “Reportable Cyber Security Incident” will allow Registered Entities the opportunity to meet the standard in a clear and measurable way. See below for alternate definitions that clarify the meanings and alleviates ambiguity contained within the current proposed definitions. Notably, Southern Company does not agree with the proposed definition of “Reportable Attempted CSI” (RACSI). The new defined term still fails to establish the parameters for what is “reportable” and should focus solely on the threshold that turns a CSI into a Reportable Attempt. If the definition of CSI is substituted where used within RACSI, it is very unclear. We suggest that this definition not have a subject of “Cyber Security Incident” since it appears that the RACSI definition is a repeat of CSI minus PSPs. We suggest that instead of repeating most of the definition of CSI and also using the CSI term as the subject, this definition should instead focus solely on the *threshold* that turns a CSI, which already includes attempts, into a Reportable Attempt. Southern Company proposes the following alternate definitions for use in CIP-008:

Cyber Security Incident – "***an unconfirmed*** malicious act or suspicious event ***requiring additional investigation to determine if it:***

- Compromis***ed***, or was an attempt to compromise the ESP or PSP, or
- Disrupt***ed***, or was an attempt to disrupt the operation of a BES Cyber System ***or associated EACMS***"

Reportable Attempted Cyber Security Incident – "a ***confirmed*** malicious act that:

- Was ***determined by the Responsible Entity to be*** an attempt to compromise the ESP, or
- Was ***determined by the Responsible Entity to be*** an attempt to disrupt the operation of *a* ***high or medium impact*** BES Cyber System ***or associated EACMS****."*

Note: Once confirmed by the Responsible Entity, the incident must be reported within the prescribed timeframes.

Reportable Cyber Security Incident - a ***confirmed*** malicious act that has compromised or disrupted one or more reliability tasks of a functional entity.

* See comments in our response to Q2 regarding the creation of a new NERC defined term "EACS".

Using the above definitions, CSI is an event that appears to potentially be malicious or suspicious and must be investigated further as per existing requirements. Once a determination is made that the event was actually targeting or attempting to compromise a BES Cyber System, or associated ESP or EACMS (for high and medium impact BCS), the event then falls into one of the two reportable categories depending on the level of success in the attempted or actual compromise, and the impact classification of the compromised asset(s). The proposed modifications shown above maintain proper scoping of reporting "attempts to compromise" at the high and medium impact BCS and associated EACMS level and does not impact the current use of the CSI and RCSI defined terms as they apply to CIP-003 R2, Attachment 1, Section 4.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends the proposed definition for Reportable Attempted Cyber Security Incident be expanded to include disruption or attempted compromise of Physical Security Perimeters and Physical Access Control Systems. This would allow identifying a Facility as a potential target without its reliability or operations being affected.

Reclamation also recommends removing the following language from the bullet point for EACMS because it is redundant of the EACMS definition: *"that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

Therefore, Reclamation recommends the proposed new term be changed

from:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

to:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter (ESP); or
- Physical Security Perimeter, including locally-mounted hardware or devices; or
- Physical Access Control Systems (PACS); or
- Electronic Access Control or Monitoring System (EACMS).

If the above solution is not accepted, Reclamation asserts the following:

The proposed definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report excludes PSPs. For example, if a PSP was breached and no BES Cyber Systems were compromised, then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

The Reportable Attempted Cyber Security Incident definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter. If the intent is to only report incidents that actually compromise cyber equipment, Reclamation recommends the Cyber Security Incident definition be changed to:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reclamation also recommends removing “Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,” from Requirement R4 Part 4.1 so it reads:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

2. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? If not, please provide comments and an alternate approach to addressing the directive, if possible.

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
While Xcel Energy agrees with adding EACMS to the Applicable Systems column in the Requirement tables, we would like to express our concern with the effect of adding certain monitoring and alerting systems as applicable EACMS. If we are required to monitor our monitoring systems for Cyber Security Incidents and Attempted Cyber Security Incidents, then shouldn't we also need to monitor that monitoring system? It is not clear to Xcel Energy where the line of succession for reporting on monitoring and alerting systems would conclude. The addition of monitoring systems creates a "hall of mirrors" effect. Xcel Energy asks the Standard Drafting Team to address the hall of mirror issue with appropriate language in the Requirement.	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	Yes
Document Name	
Comment	

We agree that adding EACMS is a step in the right direction.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree that adding EACMS is a step in the right direction

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Texas RE agrees with the addition of EACMS to the applicable systems column in the tables in CIP-008-6. Please see Texas RE's comments to question #1 regarding the definition.

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5;	

Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	

Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Reclamation recommends the SDT use existing terms from the NERC Glossary or follow procedures for adding new terms to the NERC Glossary of Terms. Instead of stating the EACMS example in the requirement, the EACMS definition should be revised as follows: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems. *Examples include Cyber Assets that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern Company feels the unnecessary inclusion of cyber assets that are used solely to perform a "monitoring and alerting" function is an undue burden to entities as they have been confirmed to have little to no impact on BES reliability. In NERC's comments to FERC in response to the associated FERC NOPR, NERC stated[1]: *"Additionally, as the term EACMS covers a wide array of devices that perform different control or monitoring functions, the various types of EACMS present different risks to BES security. As such, it may be necessary to differentiate between the types of EACMS to ensure that any reporting requirement is scoped properly. NERC thus respectfully requests that the Commission provide NERC the flexibility to define "attempts to compromise" and differentiate among EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities."* *"given the wide array of EACMS, it may be beneficial to limit the types of EACMS subject to any reporting requirement to scope the requirement appropriately."* *"while NERC is supportive of the general scope proposed by the Commission, NERC recognizes that there is still a need to refine the scope of the proposed directive to ensure that it would provide meaningful data without overburdening entities. NERC identified at least two items that require additional focus."* *"Second, as defined in the NERC Glossary, EACMS include a wide variety of devices that perform control or monitoring functions. The risks posed by these various systems may differ substantially. It is important to focus industry resources on higher risk systems. Certain devices that qualify as EACMS*

may have no or minimal impact on the security of BES Cyber Systems if compromised. NERC thus needs to consider whether to define the reporting threshold to differentiate between the various types of EACMS for reporting purposes."

"For these reasons, NERC respectfully requests that the Commission provide NERC the flexibility to refine the thresholds for reporting, including defining "attempts to compromise" and differentiating between EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities."

Despite FERC's position and language used in the Final Order, Southern feels additional discussion is needed between NERC and FERC to avoid unnecessarily scoping in systems that, if compromised, do not have a direct impact on the BES. Failing to realize this fact could hinder existing NERC SDT efforts in the realm of development of new requirements to address virtualization and other technological advancements.

Southern Company supports the Project 2016-02 SDT that is also working on redefining the EACMS definition to address virtualization and other technological advancements, and we strongly encourage the Project 2018-02 SDT to work together with them on this. Working on establishing this alignment between SDTs now will help alleviate the need in the future to modify standards again.

[1] NERC Filings to FERC DL_NERC_Comments_Cyber_Security_Incident_Reporting, Page 2, Paragraph 1.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

While Vectren agrees that adding EACMS to the scope is a good security practice, it is not clear how entities would meet the requirement without a more focused definition of Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

David Maier - Intermountain REA - 3

Answer	No
Document Name	

Comment

Applying this as reportable only to EACMSs implies that an *attempt to compromise* an EACMS is reportable but an *attempt to compromise* a BCA is not. "Attempt to compromise" must be defined and mitigating controls and monitoring should be applied to all assets and in uniform fashion.

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Add the list of functions noted in the FERC order, to define the in-scope terms. The FERC Order as follows: “and their associated EACMS that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.” We appreciate that this FERC clarification is in the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident. However, requirement part 1.1, for example, is only about Cyber Security Incidents for which the definition does not contain this FERC clarification. Therefore, as proposed, the scope of EACMS is different for this requirement part. For consistent scoping, the five functions should be added to the EACMS reference in all of the CIP-008 requirements’ applicable systems.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
While Vectren agrees that adding EACMS to the scope is a good security practice, it is not clear how entities would meet the requirement without a more focused definition of Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	

Comment
GSOC is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, GSOC believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. GSOC urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	

Comment
Agree with NPCC comments

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We are concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, we believe that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. We urge the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, NRECA believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. NRECA urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No

Document Name	
Comment	
The proposed changes and new definitions should be confirmed prior to expanding the reporting requirements to additional assets.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
This reference to EACMS also should include the five functions described in the FERC Order as follows: “and their associated EACMS that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.” We appreciate that this FERC clarification is in the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident. However, requirement part 1.1, for example, is only about Cyber Security Incidents for which the definition does not contain this FERC clarification. Therefore, as proposed, the scope of EACMS is different for this requirement part. For consistent scoping, the five functions should be added to the EACMS reference in all of the CIP-008 requirements’ applicable systems.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP recommends an adjustment from ECAMs to EAC systems because monitoring systems are not as critical and having the ECAMs monitored by a separate system will incur additional costs and resources.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	No
Document Name	
Comment	
Definitions should not include EACMs. Every packet denied by a firewall would generate a potential Reportable Attempted Cyber Security Incident, making this requirement onerous for the entities.	
Likes 0	
Dislikes 0	
Response	

3. Do you agree with reporting timeframes included Requirement R4? If you disagree please explain and provide alternative language and rationale for how it meets the directives in FERC Order No. 848.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

TVA agrees with the proposed reporting timeframes only if the definition of “attempted” is appropriately clarified based on TVA’s comments to Question 1.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Assuming there is no measurable impact on risk, I recommend updating R4.2 and R4.4 from 5 days to 7 days, so that updates could be made on a weekly basis. I recognize these reports are not intended to be a regular occurrence, but also recognize that the reporting frequency could support this consideration.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Assuming there is no measurable impact on risk, we recommend updating R4.2 and R4.4 from 5 days to 7 days, so that updates could be made on a weekly basis. We recognize these reports are not intended to be a regular occurrence, but also recognize that the reporting frequency could support this consideration.	
Likes 0	
Dislikes 0	

Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Please see comment on #4, below, regarding risk for meeting the 1 hour reporting deadline. For Reportable Attempted Cyber Security Incidents, we suggest the deadline is changed from the next calendar day to the next business day.	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	

Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC agrees the reporting timeframes are reasonable; however, because Reportable Attempted Security Incidents constitute a condition where security controls operated as designed and prevented an actual compromise or disruption, ATC supports further SDT consideration of a longer timeframe for preliminary reporting of Reportable Attempted Security Incidents to balance the risk, timely reporting, and administrative burden. Additionally, where the term 'calendar day' is used, ATC requests the SDT consider adding the qualifier, of '11:59 pm local time' for ultimate clarity on the reporting deadline.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
The companies recommend replacing "5 calendar days" with "5 nonholiday weekdays." The recommendation is to avoid required follow-up reporting to fall on a weekend or holiday.	

Also, we do not believe occasionally extending a follow-up reporting period to seven or eight days is detrimental to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees that the time for reporting a Reportable Attempted Cyber Security Incident should be different from that of a Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
This is reasonable and adds flexibility because the requirement makes it clear that 1) the timeframe is based on when the incident is determined to be reportable and 2) attribute information does not need to be submitted until it can be determined. Also, the requirement lets entities update attribute information when revised information becomes available.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

NC	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	

Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy believes that reporting updates stemming from a Reportable Cyber Security Incident would be better reported on a weekly (7 calendar days) basis after the initial notification. Entities will learn additional details of a Cyber Security Incident as the investigation evolves over time. Reporting each new item learned each time it is learned would create an administrative burden. Gathering information and reporting over 7 calendar days would allow for a more uniform internal process and regular timely reporting.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
There is ambiguity in when the reporting timeframes begin. Additional language should be added that clarify that the timeframes do not begin until the entity has concluded it's investigation and made a determination on the attempt or actual penetration. The current language could be interpreted differently and could lead to inconsistent results in determining when an attemptm or actual penetration should be reported.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
Seminole does not agree with the inclusion of EACMs in R4. See comments above.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
SRP agrees with the 1 hour and 1 day for initial reporting. Reporting if attributes change within 5 days will add administration burden of having the template attachment completed. SRP recommends an adjustment to when the investigation is complete so a complete investigation with all the facts are presented in the template attachment. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No

Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	

Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

Requirement parts 4.2 and 4.4 reference 5 calendar days. We recommend replacing 5 calendar days with 7 calendar days so this can be a regularly scheduled check for updated attribute information on the same day of the week, particularly if multiple updates are required.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No

Document Name	
Comment	
Updates within a prescriptive five calendar day or other period when attributes change or are known to E-ISAC present an unreasonable expectation on an entity. Initial reporting and final reporting upon conclusion of analysis of determination of all attributes on the entity's timeline should be the preferred basis.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
Based on our comments for question 1 to revise the existing Reportable Cyber Security Incident rather than creating an additional one, the timeline can be the same as before.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
The language, "And Reportable Attempted Cyber Security Incidents" should be removed from R4.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No

Document Name	

Comment

It is recommended that all reporting timelines fall in line with established Reporting Procedures established by current federal reporting guidelines see US-CERT Federal Incident Notification Guidelines.. ALSO: Reclamation agrees with the proposed reporting timeframes.

Reclamation recommends the following language be deleted from R4 Part 4.1 when the definition of Reportable Attempted Cyber Security Incident is modified to include PSPs: *"Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter …"*

Therefore, Reclamation recommends R4 Part 4.1 be changed

from:

Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

to:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

The one-hour timeframe for Reportable Cyber Security Incidents seems ressonable because they are critical events. However the "end of next calendar day" requirement for Reportable Attempted Cyber Security Indicents seems unnecessarily stringent. Because attempted incidents are not critical events, changing the timeframe for them to "end of next business day" would allow Entites to meet the intention of the reporting requirement without the need for additional resources to review, analyze, and report on non-cricital events that occur on weekends and holidays.

Likes 0	

Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	

Comment
We strongly encourage NERC and the SDT to reconsider requiring each Responsible Entity (RE) to report to two different agencies (E-ISAC and ICS-CERT). If NERC cannot coordinate with both agencies to have one central reporting mechanism, we would recommend expanding the timeframe to allow for one hour per agency, which would change the R4.3 requirement to: *"Timeline for initial notification: **Two hours** from the determination of a Reportable Cyber Security Incident. **48 hours** after determination of a Reportable Attempted Cyber Security Incident."* Rationale behind this suggestion can be illustrated with the following example: If an RE decides to contact the E-ISAC as the first agency and makes a phone call for initial notification, but is placed on hold for an extended time, it is possible that reporting to the ICS-CERT (as the second agency) may fall outside of the one hour window. We believe that by doubling the reporting agencies REs should receive double the amount of time to report.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The timeframe for Reportable Attempted Cyber Security Incidents could extend to almost a 48 hr period. As a reportable attempted incident, 48 hours is quite a long time and shortening this window could help EISAC increase responsiveness across regions or entities that could also be impacted. RF recommends the SDT consider revising the timeframe to be the same as or within 24 hrs from determination of Reportable Cyber Security Incidents. For example, if either event reaches the threshold of "reportable", it is recommended to have the same notification window—for consistency, ease of understanding and also to enable the industry to be proactive and prevent a potential incident from becoming an actual compromise. Why have 2 different timeframes based on the definitions between "confirmed" and "attempted"? Also, from a entity perspective, it would be easier for them to have "one" reportable notification process and timetable rather than splitting hairs based on definitions. And, most entities would likely utilize a singular notification process and report it under the same time and conditions because they wouldn't want to wait or have to create and follow separate processes.

Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA does not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agree with APPA's comments. In addition, we are concerned with the formatting of the timeline list. Tyically, bullets indicate an "or" statement, but the way the items are phrased indicates "and". If "or" is the intended phrasing, we propose the following change: Timeline for initial notification: • One hour from the determination of a Reportable Cyber Security Incident; or • By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

We do not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6

Answer	No
Document Name	

Comment

Section 4.3 – Next calendar day seems very aggressive. Would it be better to align this with the 15 day requirement currently used in other NERC CIP documents

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

More time may be needed to support a more complete investigation. Complex incidents will probably require more than five calendar days

We request clarification on “attempt” in Reportable Attempted Cyber Security Incident. Our answer to this question depends on the interpretation of “attempt” in the new term Reportable Attempted Cyber Security Incident. Attempt can be broadly interpreted so that an Entity could be constantly submitting this notification.

Likes 0	
Dislikes 0	

Response

Scott McGough - Georgia System Operations Corporation - 3

Answer	No
Document Name	

Comment
GSOC does not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
A reporting timeframe of one hour is unreasonably short due to the details requested and various organizations required to receive the reports.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	

Comment
Duke Energy suggests that 7 calendar days to submit any new or changes in attribute information is more reasonable. Having a full week to further investigate and submit any new or changed attribute information could reduce the number of subsequest reports, as well as reduce hardships if an attempted incident is discovered on or near a weekend. Also, the language used in R4 could likely create confusion or unnecessary work in order to identify when to make subsequent reporting or when to stop reporting on any one incident. We suggest that there be some language in the requirement that gives a responsible entity the ability to determine when there is sufficient information to file an update on an initial report. Example language could include: *“Once entity determines that there is sufficient information to make subsequent reporting, it should be reported within 7 calendar days.”*

Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	No
Document Name	
Comment	

Does the requirement for Reportable Attempted Cyber Security Incident imply a need to maintain staff in the event an attempted attack occurs off business hours? Perhaps this could be changed to “within 1 business day” rather than 24 hours.

Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	
Comment	

FMPA agrees with the following comments submitted by APPA:

Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in some instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day time frame.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	
Comment	

See comments in question 1.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	Revisions to R4.4.docx

Comment

AZPS is concerned that a timed obligation to update information could lead to the reporting of unverified information that could continue to change and evolve as an investigation progresses. Such could result in regulators and the industry expending efforts that would later have little to no security or reliability value or benefits. In addition to the limited and potentially detrimental value in which such updates could result, the timing requirements of R4 divert resources from more important tasks such as containment, remediation, and forensic investigation. This seems unduly burdensome and AZPS recommends that the continuous update requirement be re-considered. Nonetheless, AZPS supports the maintenance of a reporting obligation until all attributes have been completed and submitted.

To address the need for ongoing reporting until all attributes are complete, AZPS recommends that any attributes not originally reported in Attachment 1 pursuant to requirement R4.3 be reported within 5 calendar days of the conclusion of the Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. AZPS believes this timing is appropriate as it ensures that information that is reported and/or shared is actionable and accurate and that resources remain focused on the Cyber Security Incident until its containment and remediation is completed.

Additionally, AZPS notes that attributes initially reported could change as the investigation progresses and therefore recommends that, if there is change to an attribute that was previously reported, such updates should be reflected in the final report for notification. If the result of the Cyber Security Incident investigation indicates that an attribute is unknown, such should be reported in the final report.

AZPS recommends the language change to R4.4 shown in the attached.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	

Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Stated in R4.2 & R4.4., suggested to update every seven (7) calendar days, not every five (5). This can be a regularly scheduled check for updated attribute information on the same day of the week, particularly if multiple updates are required.	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	No
Document Name	
Comment	
Luminant has concerns about the ability to meet the one-hour horizon for all three agencies that require reporting within an hour (E-ISAC, ICS-CERT and DOE). Additionally, this activity distracts from actual response activities. We do understand the value of quick reporting, especially if there is a coordinated attack that involves multiple entities. Reducing the reporting requirement back to a single report that is automatically disseminated to all relevant agencies would resolve this concern.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

Timeline for initial notification of attempted is unreasonable at next calendar day (ie Friday or Saturday evening event). Additional days should be allowed to support a more complete investigation.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in all instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day timeframe.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	

Response

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5

Answer	No
Document Name	

Comment

Tacoma Power agrees with APPA comments:

"Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in some instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day time frame.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame."

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Regarding timing, APPA is concerned with the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident.” Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always fit in the end of the next calendar day time frame.

We are also concerned over the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We believe that it is too difficult for the entity to report an Attempted Cyber Security Incident in the next calendar day without a more refined definition of Attempted Cyber Security Incident. Furthermore, investigations into attempted cyber security incidents can span days or weeks. Notification in the early stages of the investigation does not provide the level of detail that would make the notification valuable to the E-ISAC and ICS-CERT or registered entities.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

FERC Order No. 848 Paragraph 89 contemplates three timeframes for reporting:, which are summarized below:

- **1 hour - Detected Malware within ESP or incident that disrupted reliability tasks**
- **24 hours – Detected attempts at unauthorized access to an ESP or EACMS**
- **Monthly –Other suspicious activity associated with an ESP or EACMS**

The proposed language captures the 1 hour and 24 hour timelines, but omits the suggested monthly timeline. SCE&G recommends revising R4.3 as follows:

“Timeline for initial notification:

- **One hour from the determination of a Reportable Cyber Security Incident.**

- **By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident *that consisted of multiple targeted attempts to access an ESP or EACMS or to disrupt a reliability task.***

- ***All other Reportable Attempted Cyber Security Incidents shall be aggregated and reported once each calendar month*.” (The SDT should develop another attachment for this reporting.)**

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC

Answer	No
Document Name	

Comment

More time may be needed to support a more complete investigation. Complex incidents will probably require more than five calendar days

We request clarification on “attempt” in Reportable Attempted Cyber Security Incident. Our answer to this question depends on the interpretation of “attempt” in the new term Reportable Attempted Cyber Security Incident. Attempt can be broadly interpreted so that an Entity could be constantly submitting this notification.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam

Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Attempted CSI should have a reporting deadline not sooner than the end of the next business calendar day.

The proposed language of R4.1 excludes any CSI that includes a physical component, even if it also has a cyber component. This is likely not intended.

Also, the Reportable Cyber Security Incident term by definition does not include PSP attracts. Why does the language of R4.1 suggest it does?

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The timeline for a Reportable Attempted Cyber Security Incident should not be the next calendar day. More time is often required for registered entities to provide useful information to share for an attempt, and such sharing will still be timely even if not the next day. If the objective is to improve registered entity situational awareness it would be prudent to allow for multiple days to support more complete investigation. Based on an interest in complete information in the report and concern regarding needed resources to investigate attempted compromises there should be a longer timeline in such cases.

The timelines for reporting to both the E-ISAC and ICS-CERT are overly complicated. The requirement of additional reporting for attempts and updates do not provide significant value for the E-ISAC, the ICS-CERT or registered entities.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	No
Document Name	
Comment	
Exelon suggests increasing to a 4-hour reporting timeframe for Reportable Cyber Security Incidents to permit greater focus on incident response and allow additional time to facilitate reporting.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The one hour timeframe for initial notification is consistent with CIP-008-5. “End of the next business day” for Reportable Attempted Cyber Security Incident seems reasonable and would allow for E-ISAC and and ICS-CERT to have reasonale awareness. As for the updates with 5 calendar days, this seems like a reasonable timeframe, but recommend the SDT revisit the language in Part 4.1 and 4.4. The wording between the two Parts could use further clarity.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
It is unrealistic to think that small entities have adequate staff on hand to continuously update multiple organizations about attempted cyber attack. Furthermore, a lack of coordination between E-ISAC and ICS-CERT (DHS) is not the industry's fault. Reporting to one entity should be sufficient for responsible entities.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company is concerned that the emphasis in these requirements is shifting from maintaining a reliable BES toward a focus on collecting and reporting data. This detracts from registered entities' obligation to maintain their focus on the reliable operation of the BES.

In reviewing R4, Southern Company the following clarification in the proposed Standard to more clearly address "who makes the determination." That said, we recommend in R4.3:

Timeline for initial notification:

- One hour from the **Responsible Entity's** determination of a Reportable Cyber Security Incident.
- By the end of the next calendar day after a **Responsible Entity's** determination of a Reportable Attempted Cyber Security Incident.

And in 4.4:

Responsible Entities shall submit Attachment 1 updates for the attributes required in Part 4.1 within **7** calendar days of **the Responsible Entity's** determination of new or changed attribute information. Submissions must occur each time new attribute information is available until all attributes have been reported.

As shown above, Southern Company also recommends the "update timeframe" in R4.4 to be expanded to 7 calendar days to facilitate regular and timely reporting for issues of an extended duration. Doing so will facilitate the ability for a registered entity who experiences a need to update attribute information to do so on a regular weekly schedule until all attributes have been reported.

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that all reporting timeframes align with reporting procedures established by federal reporting requirements, such as DHS/US-CERT Federal Incident Notification Guidelines.

When the definition of Reportable Attempted Cyber Security Incident is modified to include PSPs (as stated in the response to Question 1), Reclamation also recommends R4 Part 4.1 be changed

from:

Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

to:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

4. The SDT created Attachment 1 to be used for consistent reporting and intentionally aligned the content with FERC Order No. 848 paragraphs 69 and 73. Do you agree with the content and use of Attachment 1?

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

Recommend a reference to the NERC Glossary for identifying the Incident Type.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy believes that it is unclear if the Responsible Entity also needs to be identified or just the name of the person submitting the notification in Attachments 1 & 2

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

Exelon agrees with the form, but offers suggestions for improvement. Some considerations for scenarios when considering revisions to the form:

- Suggest addition of a field or explanation for indicating a report is the final.
- Should the form include where the incident is occurring?

- Should the time of the occurence be included on the form so other RE's could potentially assess for potential threats, on their system, around the same time as well?
- Adding information to include how/where to submit the information (ie. Email, phone number).

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

Reporting to multiple agencies using different forms/formats should be avoided to reduce redundancy and burden on the entities.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy

Answer	Yes
Document Name	

Comment

Entities currently have several agencies, each with their own form, to report to in the event of a Cyber Security Incident. Many states now also require reporting with their own form, and more states are following suit. The SDT should consider coordinating with other agencies, such as the DoE, to consolidate to a single form. Unique forms for each agency introduce considerable risk for meeting the reporting deadline.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

We suggest the following changes to the format and content of the form:

Attachment 1 appears to require the first and last names of the primary point of contact, but the form never requests the name of the Responsible Entity. We would suggest including a box that asks for this information.

Additionally, the “Required Attribute Information” fields should parallel the order in the Standard for consistency. “Attack Vector” should be listed second, and “Functional Impact” should be listed first.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

No Comment

Likes 0	
Dislikes 0	

Response

Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	
Comment	
Recommend Required Attribute Information should have more specificity. Expect the industry will want to see trending over time. Does the Entity still need to submit an EOP-004 or 417 in addition to the Attachment 1? Concerns regarding information protection when submitting Attachment 1	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
However, please reference BPA’s response to Question 1 regarding “attempt.”	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	

Comment
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1	
Answer	
Document Name	

Comment
Abstain. ATC agrees with the content of Attachment 1 will meet FERC directives, and understands the SDT labored about how to keep it both simple and useful. ATC believes there may be opportunity to share better information and further minimize risk and exposure to the Bulk Electric System if this included some mechanism for timely and secure sharing of additional pertinent (and optional) details as like indicators of compromise, detection mechanism, and exploits used/vulnerabilities exploited. ATC requests the SDT reconsider whether the use of Attachment 1 must be a requirement.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Texas RE seeks clarification on whether or not Attachment 1 is required for reporting. Requirement Part 4.2 does not explicit say entities must submit Attachment 1 for all notifications. Texas RE recommends adding an additional comment box to Attachment 1 for the entity to provide any additional information that does not specifically align to the three attributes.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy does not agree with the use of Attachment 1, as if NERC requires the use of the Attachment for notification, then it should be referenced in the Requirement language. NV Energy would request the SDT revise the language to allow any form of an electronic document/evidence by the notifying entity that includes 1) The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted. This would be in lieu of making Attachment 1 a required submittal.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council.	
Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that “Attachment 1” not be included in any requirement. Incident reporting should follow published methods already defined by the DHS Federal Incident Notification Guidelines. Only one reporting form should be used for all incident reporting, including CIP-008 and EOP-004. Multiple different forms (CIP-008 Attachments 1 and 2; EOP-004 OE-417 and Attachment 2, etc.) create confusion and provide opportunities for errors and omissions.

Reclamation also recommends CIP-008 Requirement R4 Parts 4.2 and 4.4 be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism. The language requiring submission of Attachment 1 within 5 days should be withdrawn because it potentially creates an unnecessary paperwork burden on entities, especially if the E-ISAC provides a more efficient mechanism to maintain this information in the future (e.g. a webpage, etc.).

Additionally, Reclamation recommends Requirement R4 Parts 4.2 and 4.4 include an exception for CIP Exceptional Circumstances and for situations when E-ISAC is unable to accept notifications.

Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company disagrees with the proposed options for reporting, and recommends the SDT focus on the “what” and not the “how” of the requirements. For example, the Standard does not currently allow for advancements in automated data processing where web reporting services could be used to allow for automation of reporting and the updating of submitted information.

In FERC Order 848, FERC states[1],

“We also support the adoption of an online reporting tool to streamline reporting and reduce burdens on responsible entities”

Southern Company agrees with this statement as well as FERCs assertion that a Section 1600 data request is inappropriate for this type of information reporting. Aligned with this belief, Southern Company contends the ultimate goal of “attempted incident reporting” is to share indicators of compromise attempts at machine speed in the future. We do not agree with prescribing that this be must done by a particular form filled in by humans. While this

may work in the short term, the future goal should be to move beyond this manual process as technology allows, making the requirement obsolete due to its overly prescriptive method.

Additionally, we affirm that the standard should be results-based and not prescribe a manual form be used. If something needs to be changed on the form in the future, NERC will need to stand up a SDT, ballot the changes with industry, and file with FERC. Experience shows that it will take a year or more to make any change to the form. The SDT should consider that any guidance on "how" the required elements may be reported is better covered in Implementation Guidance. The recipients of the data may desire to design web interfaces or web services in the future for the submission of this data. If E-ISAC or ICS-CERT design something within their portal for ease of submission and ingestion of this data, we believe the proposed requirement to use a form is unwarranted and counterproductive.

[1] FERC Order No. 848, *Cyber Security Incident Reporting Reliability Standards* ¶ 61,033 (2018), Docket No. RM18-2-00, Page 58, Section 91

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Would strongly prefer to see it merged with OE-417.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The approach to reporting should be related to a reporting process agreed to by both E-ISAC/ICS-CERT as opposed to use of a form. We should try to avoid specifying technology versus outcomes. Should this simply be left with notification to groups as opposed to specifying means – given an incident may remove one or more means for reporting (i.e. internet access disconnect or similar measures during an incident)?

Regarding the form in Attachment 1, this could instead be specification of a schema for reporting that could be incorporated into a portal or similar reporting process as determined by E-ISAC (and/or ICS-CERT). The standard should be technology independent as much as possible. The standard

should speak to responsible entity concerns regarding the information sharing classification of this sort of report for E-ISAC and ICS-CERT (TLP of some sort, PCII, how does FOIA get involved?).

Regarding contact information required for the form in Attachment 1, there should be provision for an alternate contact to support operational contacts. The standard should clarify whether this is meant to be a compliance contact or an operational (cyber) contact. The standard should address expectations for access to a contact (24 by 7, next business day, etc.) by E-ISAC/ICS-CERT during an investigation so entities can select appropriate contacts and ensure responsible parties provide reasonable response in such cases

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC

Answer	No
Document Name	

Comment

We recommend “Required Attribute Information” should have more specificity. Expect the industry will want to see trending.

Does the Entity still need to submit an EOP-004 or 417?

What about information protection when submitting?

We recommend that directions to filling out Attachment 1 should point to Attachment 2.

We recommend that this form and the means to submit should be more technically agnostic.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

Overall, the reporting form provided in Attachment 1 is good and aligns with FERCs Order. However, the CIP-008 reporting requirements need to be reviewed in concert with EOP-004 and OE-417. The overlap in these requirements creates multiple reporting thresholds and multiple dissimilar reporting timeframes and forms. This overlap will create confusion and will be burdensome for entities to manage. There will also be inconsistencies between what is reported by entities on the OE-417 form versus CIP-008 Attachment 1.

To address this overlap, SCE&G recommends EOP-004 be revised to omit CIP-008 Applicable Systems, since these assets are effectively be covered by the CIP-008 Standard. NERC should work with the DOE to develop a process to share information provided by entities in CIP-008 reports.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provided Entities with an option to notify a number of different organizations. An option would be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities should not be encumbered with duplicative portals, email addresses and telephone numbers to track for reporting.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The requirement (R4.4) to use Attachment 1 for reporting should be eliminated. Use of the form is a cumbersome manual process that will put unnecessary constraints on the ability of entities to report. This is likely to be especially true in the case of Reportable Attempted Cyber Security Incident which, depending on interpretation, could number in the hundreds per day. No one has a good idea of how many reports will be necessary now or, especially, in the future. Requiring use of Attachment 1 would put an administrative burden on reporting entities and hamper the ability of entities, E-ISAC and ICS-CERT to develop automated reporting tools and processes. The Standard should concentrate on the security objective and not specify how it is met. Attachment 1 could be included in a guidance document as an optional way of complying. Alternatively, use of the form could be a recommendation from E-ISAC and ICS-CERT.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The standard is not clear on how to report an incident that was an attempt to compromise or a compromise to the PSP. The standard clearly states not to use Attachment 1 for this. It's easier for Registered Entities to use one form for all Reportable Cyber Security Incidents. Recommend that Attachment 1 include information for reporting attempts to a PSP.

Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting."

Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

APPA appreciates the SDT's efforts to ensure consistent reporting in compliance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we have concerns about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Required use would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information today to organizations such as E-ISAC and ICS-CERT. Moreover, duplication or restating existing reporting is not efficient and obligating the industry to use the proposed form would obstruct the creation of more efficient reporting mechansims. Also, use of the proposed form would be complicated by unintentional omissions or mistakes that could result in compliance violations, leading to inefficient use of resources by both entities and the ERO. Because of these concerns, APPA recommends that Attachment 1 not be required, but rather be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

The requirement (R4.4) to use Attachment 1 for reporting is a cumbersome manual process that will put unnecessary constraints on the ability of entities to report. Based on current reporting, Reportable Attempted Cyber Security Incidents which, depending on the definition and its interpretation,

could be hundreds per day and could increase in the future. Requiring use of Attachment 1 would put an administrative burden on reporting entities and as mentioned above, constrain complying entities, E-ISAC, and ICS-CERT from developing better automated reporting tools and processes. APPA recommends that the Standard focus on the security objective without specifying a specific form. Attachment 1 can best be provided as a guidance document, or as something that complements existing E-ISAC and ICS-CERT reporting.

APPA believes that any new form (required or not) should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	No
Document Name	

Comment

The companies have three suggestions:

1. Add “BES Cyber System Information” to the Attachment 1 header and language addressing information protection;
2. Add language to the form that provides flexibility to E-ISAC and ICS-CERT to develop an alternative format for submission; and
3. Add an “incident identifier” field.

1. Adding “BES Cyber System Information” (BCSI) to Header

The companies recommend adding “BES Cyber System Information” to the Attachment 1 header and the following statement in the body of the form:

“The information contained in Attachment 1 may include BES Cyber System Information (BCSI) and FERC defined Critical energy infrastructure information (CEII) (18 C.F.R. § 388.113). Registered Entities shall protect disclosure of Attachment 1 information except as required by FERC Order 848.

Disclosure of information contained in Attachment 1 is with limitation and shall not be disclosed except to E-ISAC and ICS-CERT in the manner as set forth under [Add citation to FERC Order 848].”

Background

The information included on the form will fall under the NERC Glossary Term, *BES Cyber System Information;* specifically, Attack Vector, Functional Impact, and Level of Intrusion.

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Also, the nature of the Attachment 1 information easily falls within the FERC definition of Critical energy infrastructure information (CEII).

"**Critical energy infrastructure information** means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

[…]

(ii) Could be useful to a person in planning an attack on critical infrastructure;

[…]"

(Excerpt, 18 C.F.R. § 388.113 (c)(2))

In addition, the case can be made there will be instances the data reported will not explicitly fall within the BCSI Glossary Term; however, we consider information regarding the volume of unsuccessful attacks "could be useful to a person in planning an attack on critical infrastructure" even in the case the information is non BCSI.

Bad actors are informed of potential vulnerabilities by a high volume of attacks, that the vulnerability may be a rich target to breach security. Of equal concern is an attacker's strategy being informed by a low volume of attempts, suggesting to the attacker to look for viable vulnerabilities elsewhere.

Either way, any information that informs an attacker's strategy "…could pose a security threat to the BES Cyber System…" and we believe treating Attachment 1 as BCSI or CEII, for that matter, while not perfect solutions, will better protect the reliability of the BES.

2. Alternative Format Language

The companies take the position that E-ISAC and ICS-CERT should have flexibility in the format of how the information is received by these organizations. It is our expectation E-ISAC and ICS-CERT would consult and agree on the same format for submitting data.

Attachment 1 is incorporated by reference into the Requirements and will be treated as required under the Standard. Since this is the case, flexibility in the format of the submission would lend itself to efficiency by not requiring changes to Attachment 1 to go through the Standards Drafting Process every time changes are needed.

The companies believe the intent of Attachment 1 and Order 848 us to provide clarity as to **what** information should be submitted to E-ISAC and ICS-CERT, not the format as to **how** it's submitted.

Accepting that as the case, we offer the following statement to be included on the form and / or other enforceable section of the Standard as the SDT may see fit:

Attachment 1 represents the required data, if known, for submission to E-ISAC and ICS-CERT. The format of the form, not the specified content, may be modified by agreement of E-ISAC and ICS-CERT.

3. Incident Identifier Field

The companies would not normally make a “process” suggestion, but should Attachment 1 be approved without an option for flexibility as to format, we recommend adding a field that provides an incident identifier for each submission so to easily identify initial and any subsequent reporting as relating to the same incident.

Though we believe E-ISAC and ICS-CERT would provide an incident identifier for each submission, we did not want to make that assumption and offer it to the SDT for consideration on Attachment 1.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	No
Document Name	

Comment

Luminant is concerned with the use of Attachment 1. Luminant understands that the SDT did not feel it was feasible to modify the OE-417, but Luminant thinks this is the only reasonable path forward. Having to complete two separate forms with significant overlap related to cybersecurity incidents but different overall objectives forces entities to focus on reporting an incident over responding to an incident. Additionally, the OE-417 has clear provisions regarding confidential information, FOIA and CEII such that an entity understands how its contents are protected and shared. The standard as currently written does not include any provisions regarding the protection of its contents or the circumstances under which it can be publicly or privately disclosed. Given the media’s inclination for hyperbole regarding cybersecurity and the energy sector, clear provisions and strong protections are critical. At the very least, Attachment 1 should be stamped CEII within the standard itself; however, Luminant is opposed to using Attachment 1 at all and prefers the SDT pursue modifications to the OE-417. Additionally, while NERC and the E-ISAC are required to follow CEII handling and protections, we are uncertain whether ICS-CERT as a division of DHS has the same constraints.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Agree that there should be minimum requirements for submission of reports and with the proposed form, but would

The suggested FORM, Attachment 1, should not be required in it's present form. Request that you add check boxes: (e.g., unknown, EACMS) rather than just a narrative piece that meet with the instructions/requirements.

Entity should be allowed to submit in ANY format, as long as the report contains the same specified fields of information. Standards **should not be technology-dependent**. Forms tend to be revised over time**. Having the Attachment 1 form as part of the standard would require another SAR to tweak the form**.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports SDT efforts to ensure consistent reporting in conformance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we are concerned about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Such an obligation would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information to the E-ISAC and ICS-CERT. Over time more automated and efficient methods of submitting this information may be created. Obligating the industry to use the proposed form would create a barrier to using such new, more efficient reporting mechansims. Moreover, any unintentional omission or mistake while using the proposed form could result in compliance violations, leading to inefficient use of resources by both entities and the ERO. To resolve this concern, EEI recommends that Attachment 1 be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
Based on AZPS's recommended language in R4.4, we recommend changing the form to include an option for "complete" and remove the option for "update".	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
Should not include "Reportable Attempted Cybersecurity Incident."	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments submitted by APPA: APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based	

reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

Follow-on reporting in Requirement R4.4 requires repeated reporting until all attributes of the event are known, but determination of attack vector, impact, or level of intrusion may be impossible to ascertain during or after the event. A qualifier needs to be added to Requirement R4.4 to only require reporting of attributes that can be determined.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

See comments from the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No

Document Name	
Comment	

We recommend “Required Attribute Information” should have more specificity. Expect the industry will want to see trending.

Does the Entity still need to submit an EOP-004 or 417?

What about information protection when submitting?

We recommend that directions to filling out Attachment 1 should point to Attachment 2.

We recommend that this form and the means to submit should be more technically agnostic

Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	
Comment	

As noted in question 1

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The addition of specific information collection data points would be helpful in more quickly analyzing and providing useful information to the industry.

Additional information to consider collecting:

- Entity's Name, NERC ID and registered function(s)
- Entity's internal tracking number (e.g. IRT Case #, Change Record, etc.)
- Timestamps including the timezone the report is being made from
    - Date/time of report
    - Date/time incident start
    - Date/timeincident detected
- Discovery Method (malware detection, operator reported suspicious activity, etc.)
- Identification of external organizations that have been notified or engaged (e.g. law enforcement, etc.)
- Define and provide common "Functional Impact" categories (critical and non-critical) as part of the reporting form for consistent reporting purposes (e.g. No impact | Minimal Impact | Significant Impact | Denial of Critical Services/Loss of Control, Destruction Impact)
- Define and provide common "Attack Vectors" or use known taxonomy as part of the reporting form for consistent reporting purposes (e.g. Unknown, Attrition, Web, e-mail/Phising, External/Removable Media, Web/IRA, Improper usage, loss or theft of equipment)

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	

While we generally agree with the content and use of Attachment 1, we would ask that NERC and the SDT consider coordinating with E-ISAC and ICS-CERT to implement an electronic version of the form for ease of initial reporting, updating, and tracking by the Responsible Entity (RE). Furthermore, if upon submission, the form could automatically route the data to both agencies, that would save the RE the undue burden of submitting twice and potentially encountering discrepancies between the two agencies during initial and updated submissions. If automation is not possible, consider adding a check box on the form indicating that E-ISAC needs to forward the report to ICS-CERT. It is our understanding that E-ISAC already works with National Cybersecurity and Communications Integration Center (NCCIC) of which ICS-CERT is one branch. This would cover the RE's responsibility to

report to both agencies when necessary, but ensures E-ISAC and ICS-CERT are coordinating any response. The electronic submission should incorporate encryption or other security measures to ensure the information remains confidential.

Also, it is unclear whether updates to the form can only include the required attribute that is being updated and all other attributes can be left blank, or if it is intended that the RE re-submit attribute information which has not changed since the last update. If it is intended to be resubmitted, would an RE check the “initial” box for that attribute, or “update” even if there was no update to that specific attribute? Depending on the intent, we ask that the SDT consider whether it is redundant to include an “initial” and “update” checkbox for each individual attribute when it is already documented in the “Reporting Category” section above. If it isn’t redundant then consider a “no update” checkbox to be added to each attribute.

In addition, in the event that the RE has reported a Reportable Attempted Cyber Security Incident, but later through additional investigation determines it was a false positive, the form does not appear to have a way to retract or withdraw the report.

Finally, in Attachment 2, under the guidance for each required attribute, it states “If not know, specify ‘unknown’ in the field.” It is unclear if “unknown” can be acceptable as a final report answer.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

Automation and JSON or XML formats should be supported for reporting events. Completing a form manually will lead to errors that affect data accuracy, which is crucial for analysis and trending.

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

WAPA does not believe that “Attachment 1” should be included in any language of the requirement. Reporting of an incident should follow published methods already defined by the US-CERT Federal Incident Notification Guidelines. The inclusion of Attachment 1 requires duplication in effort and could require entities to provide two separate forms of reporting. The US-CERT Incident Reporting System is already established and provides the necessary information and capability to report incidents.

ALSO: Reclamation recommends one reporting form be used for all incident reporting, including CIP-008, EOP-004. Multiple different forms (CIP-008 Attachments 1 and 2; EOP-004 OE-417 and Attachment 2, etc.) create confusion and provide opportunities for errors and omissions.

Reclamation also recommends Requirement 4 Part 4.2 and 4.4 be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism. The language requiring submission of Attachment 1 within 5 days should be withdrawn because it potentially creates an unnecessary paperwork burden on entities, especially if the E-ISAC provides a more efficient mechanism to maintain this information in the future (e.g. a webpage, etc.).

Reclamation also recommends Requirement 4 Parts 4.2 and 4.4 include an exception for CIP Exceptional Circumstances and for situations when E-ISAC is unable to accept notifications.

Reclamation also recommends Requirement 4 Part 4.4 specify the allowable method(s) for submitting Attachment 1 updates.

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	Attachment 1A.DOCX

Comment

Recommend redesign of Attachment 1 to align with comments for updated language of proposed modified term *Reportable Cyber Security Incident* and proposed new term *Reportable Attempted Cyber Security Incident*. See Attachment 1A.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

WEC Energy Group supports SDT efforts to ensure consistent reporting in conformance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we are concerned about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Such an obligation would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information to the E-ISAC and ICS-CERT. Over time more automated and efficient methods of submitting this information may be created. Obligating the industry to use the proposed form would create a barrier to using such new, more efficient reporting mechansims. Moreover, any unintentional omission or mistake while using the proposed form could result in compliance

violations, leading to inefficient use of resources by both entities and the ERO. To resolve this concern, WEC Energy Group recommends that Attachment 1 be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We do not believe that the reporting forms should be attachments to the standard, but rather should follow the BAL-003 model with FRS Forms 1 and 2. Using the attachment approach will require a revision to the standard in order to make minor information sharing improvements needed by the E-ISAC.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	

Comment
I do not believe that the reporting forms should be attachments to the standard, but rather should follow the BAL-003 model with FRS Forms 1 and 2. Using the attachment approach will require a revision to the standard in order to make minor information sharing improvements needed by the E-ISAC.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
We agree with the content of Attachment 1, but entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information. Standards should not be technology-dependent. Forms tend to be revised over time. Having the Attachment 1 form as part of the standard would require another SAR to tweak the form.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No

Document Name	
Comment	
No discussion of overlap or hierarchy with regards to OE-417.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
No discussion of overlap or hierarchy with regards to the OE-417.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
No discussion of overlap or hierarchy with regards to the OE-417.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP agrees with the form as an industry template for consistency. If reporting attributes change within 5 days adds administration burden of having the template attachment completed. SRP recommends an adjustment to "when the investigation is complete" so an investigation with all the facts are presented.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The content seems to be sufficient, except the definition of “Reportable Attempted Cyber Security Incident” is still unclear. What does it mean to attempt? What includes an attempt?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Entities should not be required to use a specific form through reference in a Requirement. Using a static form could preclude entities from providing appropriate information as each actual or attempted cyber incident is different, requiring specific information to be provided to be of value, and the cyber landscape continues to evolve, which may require different information to be provided in the future. The current form would be required to be used 'as is' unless the Standard was modified. An additional concern is that any omissions or mistakes in using the form could result in unecessary compliance activities, leading to an inefficient use of resources by both entities and the ERO. Dominion Energy is of the opinion that proposed Attachment 1 should either be removed or be provided only as an example and not a requirement.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

5. Do you agree with the required methods of notification proposed by the SDT in Requirement R4, Part 4.2? If no, please explain and provide comments.

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy believes the listed methods of notification are sufficient. However, there is redundancy in the language, "electronic communication" and "email", as email is a form of electronic communication. If the term "electronic communication" is preparation for an online submittal portal for E-ISAC and ICS-CERT then NV Energy believes the language is sufficient.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	Yes
Document Name	

Comment

AEP supports the methods of notification as proposed by the SDT in R4 Part 4.2. In addition we would support the idea of reporting to the E-ISAC who would then act as a conduit to other governmental agencies on behalf of the reporting entity. AEP feels this would streamline the reporting process, lessen the reporting burden on members and ensure all necessary agencies are informed appropriately.

Likes 0	

Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
NO comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA recommends that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
We recommend that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	Yes
Document Name	
Comment	
GSOC recommends that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
R4 VSL implies a preference for the use of the form for notification. If there is an order of preference for these methods, it should be clearly stated in the standard.	
Likes 0	
Dislikes 0	
Response	

Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC requests consideration of adding a ‘catch all’ in an attempt to accomplish a technology agnostic approach, and ‘future proof’ it enough so it can adapt/scale as E-ISAC and ICS-CERT processes mature and change without requiring modifications to the Standard.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	

Answer	Yes
Document Name	
Comment	
Exelon supports the methods of notification, but asks the standard drafting team to include a note in the form to request receiving entities confirm receipt or provide another method of ensuring entities receive such a confirmation.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Again, would rather not see a separate form created.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council. ERCOT also adds that it has concerns with the suggestion to email the form that may contain sensitive information. A secure submission means should be used or encrypted email.	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends reporting requirements be limited to a single destination and not duplicated between E-ISAC and DHS. Establishing communication between those organizations is not the responsibility of the registered entity. The DHS Incident Reporting System is already established and provides the necessary information and capability to report incidents.

Reclamation also recommends the SDT clarify what method of transmission is meant by “electronic submission of Attachment 1” (e.g., facsimile, web-form, etc.). Requirement R4 Part 4.4 should specify the allowable method(s) for submitting Attachment 1 updates (e.g., electronic submission, facsimile, email, etc.).

Requirement R4 Part 4.2 should be changed

from:

Responsible Entities shall use one of the following methods for initial notification:

Electronic submission of Attachment 1;

Phone; or

Email.

to:

Responsible Entities shall submit initial notification in a manner permitted by the E-ISAC, including electronic submittal, phone, or email.

Finally, Reclamation recommends Requirement R4 not require entities to notify the ICS-CERT. Replace “ICS-CERT” with the “U.S. Department of Homeland Security” instead of any specific CERT entity within DHS.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
As discussed in the previous question, Dominion Energy is of the opinion that a static form should not be used for this type of reporting and requiring Attachment 1 in both the Requirements and Measures is inappropriate. While certain information should continue to be required, the methods of notification need to remain flexible.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Revise “Electronic submission of Attachment 1” to state “Electronic submission with the specified fields of information identified in Attachment 1 to the extent known.” Remove the email option. It is redundant. Email is a form of electronic submission.	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations should occur to lessen the reporting obligations of entities.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations should occur to lessen the reporting obligations of entities.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
Please note WEC Energy Group concerns regarding Attachment 1 as described in our response to question 4.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
We agree with the required methods, but please describe how to make an electronic submission.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No

Document Name	
Comment	

Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations is not the responsibility of the registered entity. Additionally the US-CERT Incident Reporting System is already established and provides the necessary information and capability to report incidents. ALSO: Reclamation recommends the SDT clarify what method of transmission is meant by “electronic submission of Attachment 1” (e.g., facsimile, web-form, etc.).

Requirement 4.2 should be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism.

Likes 0	
Dislikes 0	
Response	

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	
Comment	

Submittal of the manually completed form is inefficient. A better solution, less prone to error is submittal of data in JSON or XML format.
Submittal via plan text email or uploading to an unsecure web site does not provide sufficient security for BCSI and other sensitive, proprietary data. Secure transfer is needed.
The current proposal to submit the same data to two organizations is inefficient and redundant.
A more efficient, secure means of notification would be via an automated solution to a single secure web site

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	
Comment	

We generally agree with the required methods outlined in R4.2, with a few caveats:

1. We believe there should only be one report necessary (and not two separate reports for E-ISAC and ICS-CERT). See previous comment for #4 regarding form modification to indicate that E-ISAC needs to forward the information to ICS-CERT.

2. It does not appear possible to submit R4.4 notification via phone (due to the use of the word “submission”). If this is not a feasible option for R4.4, it should be specified in R4.4 what notification methods are allowable. The usage of phone as a method in general should be reconsidered for practicality.

3. While electronic submission is one of the methods, we do not yet see instructions for how or where to execute this type of submission. Further guidance on electronic submissions must be provided.

4. Consider adding CIP Exceptional Circumstance exception verbiage to the second paragraph of R4.2 and split out the “without attribute” clause to be a separate sentence for clarity. This proposed modification would read “*If Attachment 1 was not submitted for initial notification, it must be submitted within 5 calendar days, except under CIP Exceptional Circumstances. Initial notification may be submitted without attribute information if undetermined at the time of submittal*.”

5. Consider moving the second paragraph of R4.2 to R4.4 for clarity.

6. R4.3 appears to be part of R4.2 and is a sentence fragment, which is inconsistent with the way other requirements are written. Consider modifications to correct inconsistencies.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6

Answer	No
Document Name	

Comment

Agree with NPCC comments

Likes 0	
Dislikes 0	

Response
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman
Answer	No
Document Name	
Comment
See comments from the MRO NERC Standards Review Forum.
Likes 0	
Dislikes 0	
Response
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE
Answer	No
Document Name	
Comment
There is a conflict between required reporting of [successful] attack vectors and safe handling of BES Cyber System Information (BCSI), or information that could be used to gain unauthorized access or pose a security threat to a BES Cyber System. CenterPoint Energy suggests that the details of how E-ISAC and/or ICS-CERT will provide verifiable records of phone reports be outlined in the requirement or guidance. Assurances that phone conversations with E-ISAC and/or ICS-CERT are confidential should also be noted in the components of this modification. CenterPoint Energy requests provisions for the security and confidentiality of phone calls, email, and electronic submissions. The SDT may consider outlining the secure methods in Implementation Guidance. For example, ICS-CERT has published a PGP public key for secure email communications. E-ISAC could consider similar secure measures. Responsible Entities need a means and assurance for the secure and confidential transfer, storage, and use of BCSI.
Likes 0	
Dislikes 0	
Response
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA
Answer	No
Document Name	
Comment

FMPA agrees with the following comments submitted by APPA:

The required methods of notification include the ICS-CERT, which does not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current Department of Homeland Security (DHS) practices. As a DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

Please note EEI concerns regarding Attachment 1 as described in our response to question 4.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment
Hard NO on submitting our reports to E-ISAC, Homeland Security & ICS-Cert separately! That would be onerous during the response to a cyber incident. Resources are needed to mitigate the incident and communicate to management. They should establish their own internal reporting much as the DOE does with the OE-417. Revise the term: 'Electronic submission,' reporting medias are: phone, email, fax…**all are forms of 'electronic' submissions**. Revise Standard language from, "Electronic submission of Attachment 1" and state, "Electronic submission with the specified fields of information identified in Attachment 1 to the extent known." **Remove the email option**. It is redundant. Email is a form of electronic submission. Regisered entities should only be required to report ONLY to E-ISAC, then the burden is on E-ISAC to forward to ICS-CERT and are self accountable, thus completing a truly confidential reporting system. This would serve to protect annionimity, and lessens the burden on the industry for reporting, thus retaining continued continuity in the information being reported. Dual reporting and dual updtates and tracking opens up the industry and the nature of the Standard, to miscommunications.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	No
Document Name	

Comment
Luminant has significant concerns regarding the current notification language. First, the bullets in 4.2 list electronic submission and email as two different methods. We are not aware of any mechanism to electronically submit the incident report to either the E-ISAC or ICS-CERT and therefore would be limited to submitting via email which offers insufficient protection for information of this nature. Second, we are opposed to submitting this information to multiple agencies. At the minimum, we will be required to submit the same form to two separate agencies and a different form to the DOE. This is administratively burdensome and focuses immediate activities on reporting rather than resolving the incident. Additionally, there is opportunity to inadvertently report information inconsistently through Attachment 1 and the OE-417 or for the information submitted to be interpreted inconsistently due to the different focus of the reports. The OE-417 has an elegant submission process that allows entities to submit information through a private and encrypted portal and also allows us to elect to send the submission to E-ISAC automatically. Anything less than this mechanism is a step backward and should be avoided. Perhaps the E-ISAC can implement a similar solution and convince the DOE to give up cybersecurity event reporting through the OE-417 in favor of receiving the E-ISAC submissions. Whatever solution is implemented, it should ensure that entities are not required to submit multiple forms to multiple agencies through multiple mechanisms.

Likes 0	
Dislikes 0	

Response

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"The required methods of notification include the ICS-CERT, which does not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current Department of Homeland Security (DHS) practices. As a DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted."

Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

The flexibility of the options for making an initial report is good. However, entities should not be required to submit Attachment 1 within 5 days. Requiring the use of a manual form for reporting cyber security incidents is an anachronism that will place expensive constraints on the development of more cost-effective tools for timely reporting. Requiring use of the form also reduces opportunities for reporting methodologies that would enhance situational awareness.

Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

The required methods of notification include the ICS-CERT that do not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current

Department of Homeland Security (DHS) practices. DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
The standard should not limit the entity to these specific forms of communication, since during an incident, these methods may not be appropriate. In addition, the standard should reflect that such information must be sent using the most secure mechanism available at the time. It may not be advisable	

for an entity to send such information using traditional email. Further, since the standard is requiring that incidents be reported to multiple entities, it may not be appropriate to limit the list of allowed contact methods.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Please see the answer to Q4.

Furthermore, Southern Company is concerned with the recommended methods of initial notification. To submit the elements of Attachment 1 via e-mail can potentially expose BCSI and other sensitive information as e-mail is inherently insecure and is plain text at the protocol level by design. Additionally, if the e-mail system has been compromised as part of an event being responded to, this method of reporting could expose information to attackers that can be used to further their agenda. The potential for disclosure of BCSI via e-mail traffic or the risk of having e-mail traffic sniffed in route makes this a prohibitive option for use and is counterproductive to reducing risk.

Submission by phone requires those who can submit this information do so from a Company phone that logs and / or records to provide the required evidence of submission, which can be costly and burdensome to entities in the wake of performing actual incident response. If this submission is performed, for example, on a personal cell phone, company personnel could be unknowingly bringing their personal data into scope of the requirements for audit purposes. This represents an undue compliance burden.

Southern reiterates its position that the requirements should focus on the “what” information is required to be reported and focus recommendations for “how” to report that information in Implementation Guidance to avoid requiring cumbersome or risky reporting methods that also severely limits the potential to develop and use an Application Programming Interface (API) for automated information submission.

Likes 0	
Dislikes 0	

Response

6. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R4? If no, please explain and provide comments.

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

Yes, however for High VSL, consider adding an additional criteria that includes failure to notify E-ISAC **or** ICS-CERT.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

NC

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	

Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation does not agree with the High VSL for R4. Recommend changing the High VSL from: The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3. to: The Responsible Entity notified E-ISAC and DHS, or their successors, but did not accomplish the initial notification within the timeframes included in R4.3. Reclamation also recommends adding the following as a third option to the Moderate VSL: *The Responsible Entity initially notified E-ISAC and DHS, or their successors, within the timeframes included in R4.3 but failed to update E-ISAC or DHS, or their successors, within the timeframe included in R4.4.*	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

NV Energy believes the VSLs for Requirement R4 are too severe for ultimately, a "reporting requirement". We believe the severe VSL should be removed for this Requirement and moved to High, thus shifting the VSL level for the other possible violations of the Requirement.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

See comments of the ISO/RTO Council.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

VSL language should provide tiered severities that reflect the true severity. As written in the draft Standard, *any* failure to report is automatically a Severe VSL regardless of the circumstances behind the failure.

Also, while it has been stated during the drafting process by the SDT that incorrectly reported information should not represent a violation, the language in the current VSL does not make this intent clear. The R4 Lower VSL currently reads (emphasis added):

*"The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident **and the attributes** within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1."*

The inclusion of "and the attributes" appears to indicate that not including the attributes (plural) is a cause for violation.

Southern Company recommends:

"The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the ***known*** attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4)

OR

The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the ***known*** attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2."

As stated previously, Southern ultimately feels that using or not using one of the prescribed methods in the current draft should not be cause for a violation if the required information is provided to the required named agencies within the required timeframes. Using a form, or an email, or a phone call, or another more technically secure and sound method should be sufficient to have achieved FERC's directives.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008

Answer	No
Document Name	

Comment

Comments: For consistency, High VSL should contain identical explanatory language as Lower and Moderate VSL.

Ex: High VSL- The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed…"

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The VSLs as defined are too focused on minor administrative details and will generate needless possible violations. Suggest instead that VSLs focus on having a process defined for reporting cyber incidents that aligns with the definition. With regard to notification methods, in a cyber incident, it is possible that traditional contact mechanisms may not be available, so Registered Entities will need the flexibility to use alternative reporting means.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	No
Document Name	
Comment	

We request clarification. At the time of determination, some attributes may not be known. Should the Entity leave that attributes blank (empty) or explicitly enter “unknown.”

We request clarification. ICS-CERT has its own process. Are Entities expected to add additional answers when submitting to ICS-CERT? If ICS-CERT changes its process, are Entities expected to follow that new CERT process when this Standard has not been updated?

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

In our opinion the prescriptive nature and detailed required reporting requirements along with the ambiguity around attempted cyber security incident definition increases the risk of a violation without adding value to stakeholders. Furthermore, the required Attachment 1 form, or other contact methods may not be available within the required reporting timeframes. Ameren recommends flexibility in both required attributes and reporting methods.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
Should not include “Reportable Attempted Cybersecurity Incident.”	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There are many issues with the language of the proposed definitions and requirements to be addressed before agreement upon VRFs and VSLs can be reached.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	
Comment	
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. GSOC recommends a Medium VSL determination for this.	
Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
We request clarification. At the time of determination, some attributes may not be known. Should the Entity leave that attributes blank (empty) or explicitly enter “unknown.” We request clarification. ICS-CERT has its own process. Are Entities expected to add additional answers when submitting to ICS-CERT? If ICS-CERT changes its process, are Entities expected to follow that new CERT process when this Standard has not been updated?

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. We recommend a Medium VSL determination for this.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. NRECA recommends a Medium VSL determination for this.

Likes 0	

Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	

Reclamation does not agree with the High VSL for R4. Reclamation recommends rewriting the High VSL as follows:

The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but did not accomplish the initial notification within the timeframes included in R4.3.

Reclamation also recommends the following be added to the Moderate VSL:

The Responsible Entity initially notified E-ISAC and ICS-CERT, or their successors, within the timeframes included in R4.3 but failed to update E-ISAC or ICS-CERT, or their successors, within the timeframe included in R4.4.

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

Given BC Hydro’s response and comments to Question #1, BC Hydro does not feel it is appropriate to comment on the associated VRF or VSL table elements.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA believes the Severe VSL should read as follows: The Responsible Entity failed to notify E-ISAC ***and*** ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	

Comment
Please modify the requirement to be aligned with the EOP-004 and OE-417 reporting requirements and reporting timeline.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Please modify the requirement to be aligned with the EOP-004 and OE-417 reporting requirements and reporting timeline.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The VSLs focus, in part, on the attributes that are reported. The attributes themselves are somewhat ambiguous and not well defined, so including the attributes in determining the severity (which may lead to monetary penalties for a Responsible Entity) of a failure to report seems to be a poor measurement for compliance.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should not result in a severe penalty.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
In general, Dominion Energy supports the VRF and VSLs with the exception of the inclusion of the requirement to use Attachement 1. Dominion Energy recommends removing all references to Attachement 1 from the VRF and VSLs.

Likes 0	
Dislikes 0	

Response

7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees	
Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
If the scope of the revisions to this standard doesn't change significantly, 12 months is acceptable.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
12 months would be adequate, not shorter.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE inquires as to whether there should be an initial performance date for Requirement Part 2.1. As written, Responsible Entities would not be required to do the first test until within 15 months after the effective date of the standard, or 27 months after the effective date of the government authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC requests the SDT consider tying the Implementation Plan and the CIP-008-6 Effective Date to the latter of 12 months or the publication of Technical Rationale and Implementation Guidance. For example: Where approval by an applicable governmental authority is required, the standard shall become effective on the latter of the first day of the first calendar quarter that is 12 calendar months after the effective date of the applicable governmental authority's order approving the standard, NERC's publication of Technical Rationale and Implementation Guidance, or as otherwise provided for by the applicable governmental authority.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
The agreement is per the understanding that this STD is further edited before issuance, and is completed correctly – then the timeine is acceptable.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
So long as an entity is in the position of defining attempts and the questions regarding reporting can be productively addressed, 12 months should be sufficient to implement the changes involved in existing programs.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	

Answer	Yes
Document Name	
Comment	
No additional comments. .	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Registered Entities who may not already have automated systems in place for alerting, logging, or detection of potential Cyber Security Incidents may need more time than 12 months for implementation of these standard changes.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Any implementation timelines can only be evaluated with specific reporting requirements.	
Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow **entities time to determine the effects of the revised** requirements and definitions, develop adequate written processes, and train personnel appropriately.	
Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole prefers an 18-24 month implementation plan in order to implement filtering and notification processes used for alerting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
To ensure a successful implementation of the revised standard, we recommend that the revised standard become effective the first day of the first calendar quarter that is **eighteen (18) calendar months** after the effective date of the applicable governmental authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
To ensure a successful implementation of the revised standard, we recommend that the revised standard become effective the first day of the first calendar quarter that is **eighteen (18) calendar months** after the effective date of the applicable governmental authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Given BC Hydro's response and comments to Question #1, BC Hydro does not feel it is appropriate to comment.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel appropriately.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
The vagueness of the definition of a reportable event makes it difficult for Entities to determine what resources will be needed to review and analyze data, how much automation to implement, etc. Entities may need more than 12 months to secure and implement the additional resources needed. Another consideration is whether the two receiving organizations will ready to receive reports within 12 months of the effective date of the new standard. What assurance that they will be ready can be given?	
Likes 0	

Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

With the additional scrutiny that attempted Cyber Security Incidents will likely require due to the modifications to this standard and associated definitions, Responsible Entities (REs) may consider modifying current network architecture for EACMS and/or Intermediate Systems for Interactive Remote Access which may currently be used for multi-impact BCS (i.e., for High, Medium, and Low impact). Splitting impacts used for each EACMS and IRA solutions may reduce investigation and reporting burden by decreasing the attack surface by taking Lows out of the equation. If this is the chosen path, additional time may be necessary for REs to initiate the supply chain and procurement processes. In which case, an 18-month implementation plan would alleviate this concern.

Additionally, with the upcoming CIP-003-7(8) Transient Cyber Asset and Removable Media malicious code risk mitigation for assets containing low impact BES Cyber Systems, it appears that by the time this CIP-008 modification goes into effect, there will be a much larger scope of cyber assets which will need to be investigated for potential Cyber Security Incidents. The impacts of this expansion may also warrant additional time for REs to adequately assess staffing and resource requirements.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

12 months is a very long period of time for implementation. The information and controls and processes for this standard should already be in place and part of a strong incident response and reporting program. The only addition is updating internal processes to submit the information to EISAC for which 12 months is a very long period of time. This should be achievable in 6 months.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No

Document Name	
Comment	
NRECA recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agrees with APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	

Comment
: GSOC recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
With the proposed definition of a Reportable Attempted Cyber Security Incident, a 12-month implementation is not reasonable. The proposed definition will require an increase in staff resources. Given the technical nature involved with tracking and investigating potential "attempts to compromise," resources are presently limited. Staff would need to be hired and properly trained to implement the processes necessary to meet the requirements. In addition, time is required to research and evaluate tools to be purchased and implemented. A minimal implementation timeframe could result in budgetary constraints or a lack of adequate resources, technology and/or tools.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
Without Technical Rationale or Implementation Guidance, entities do not have much guidance regarding classifying attempted incidents. If the standards development timeframe does not allow for specific criteria for determining "attempted," CenterPoint Energy recommends that the implementation plan be extended or postponed until after NERC has performed sufficient pilot studies to publish actionable guidance on what an attempted compromise of an EACMS looks like in comparison to normal operations of an EACMS. If the implementation plan is left as-is, entities will be required to define "attempted" events as they deem appropriate given that not doing so could possibly result in millions of reports per day or year.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy believes an Implmentation Plan of 24 months is more feasible. The proposed changes, particularly the reporting of “attempts” will bring about significant process changes, requiring the re-writing of internal procedures. Also, depending on how “attempt” is defined, the amount of dedicated workers needed to monitor and comb through large amounts of data will increase. Changes in procedures and hiring of additional workers will also require training. With anticipated procedure re-writes and additional hiring and training we feel as though an Implementation Plan of 24 months is necessary.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments submitted by APPA: The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	

Changes to the standards require Responsible Entities to make programmatic changes. Implementation plans, unless significant risks need to be mitigated in a timely manner, should allow for Responsible Entities to implement changes on their review cycle or actual events.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan."

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

The current implementation plan will require entities to change their CIP-008 as well as EOP-004 reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008

Answer	No
Document Name	

Comment

Comments: Given the interest of FERC in expediting the NERC filing, the SPP Standards Review Group believes 6 months is an appropriate timeframe for implementation.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
If not altered, the revised version of CIP-008 is not likely acheivable in 12 months. Or 24 months. It may require additional staff or an outsourced capability that requires longer look-aheads to address budget cycles.	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	
With the proposed definition of a Reportable Attempted Cyber Security Incident, a 12-month implementation is not reasonable. The proposed definition will require an increase in staff resources. Given the technical nature involved with tracking and investigating potential “attempts to compromise,” resources are presently limited. Staff would need to be hired and properly trained to implement the processes necessary to meet the requirements. In addition, time is required to research and evaluate tools to be purchased and implemented. A minimal implementation timeframe could result in budgetary constraints or a lack of adequate resources, technology and/or tools.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Given that these changes will require Responsible Entities to deploy additional resources, modify many existing security processes, potentially implement additional security controls and coordinate these changes across large enterprises, 24 months is a more reasonable timeframe for successful implementation of the necessary changes. ICS-CERT and E-ISAC may also need this time to prepare to receive and act upon this additional reporting.	
Likes 0	
Dislikes 0	
Response	

8. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

These draft standard changes could require registered entities to install additional monitoring, logging, and alerting systems to be able to acheive the necessary monitoring for adherence to this standard which would be an incremental cost.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

No additional comments. .

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the proposed revisions provide flexibility, but is concerned that the cost effectiveness and efficiency would be significantly reduced by the continual update requirements proposed within the current draft. As discussed above, there is a potential for the reporting of unverified or uncertain information or the potential taking of action by other utilities in response to non-actionable information. For this reason, AZPS has proposed its comments above, which revisions should align with the SDT's cost-effectiveness and efficiency objectives.	
Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
This may depend upon the response to question 3.	
Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Abstain	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	
Document Name	
Comment	
The proposed changes have the potential to increase work load/overtime costs for those responsible for responding to and reporting attempted incidents.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Prior to proposing additional modifications, Reclamation recommends each SDT take the necessary time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities with economic relief by allowing technical compliance with current standards.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	

Answer	No
Document Name	
Comment	
Any cost determinations can only be evaluated with specific reporting requirements.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company encourages the SDT to consider modifying the language of M4 to reflect the following:

"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* ***or evidence of active participation in an automated industry information sharing program."***

Southern Company asserts that active participation in an information sharing initiative such as the Cybersecurity Risk Information Sharing Program (CRISP) fully meets the spirit and intent of the reporting requirements outlined in FERC Order 848 and does so in an automated fashion. Technological solutions (like CRISP, DoE CYOTE, etc.) and automation are much better suited for meeting the objectives stated by FERC, where the technology itself is watching for potential incidents and sharing indicators of compromise (IOCs) across the industry in an automated fashion. These programs automatically record Cyber Security Incidents that compromise or attempt to compromise a responsible entity's ESP or associated EACMS. In NERC's publication, *Understanding Your E-ISAC* , they explain[1], "The [CRISP] program enables owners and operators to better protect their networks from sophisticated cyber threats by facilitating the timely sharing of government-enhanced threat information, enhance situational awareness, and better protect critical infrastructure." Putting forth significant additional funding and effort in expanding and maintaining the scope of manual reporting required for CIP-008 will significantly detract from our ability to fully engage in the other worthwhile information sharing projects like CRISP and CYOTE.

Southern Company would also like to reiterate that creating a double reporting burden (the requirement to file the same report to two different agencies) is onerous and ineffective.

[1] Electricity - Information Sharing and Analysis Center, Understanding your E-ISAC, (2016)

Likes 0	
Dislikes 0	
Response	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	
Identifying and investigating all potential Reportable Attempted Cyber Security Incidents would be time consuming and costly due to the resources required for these tasks. Additional staffing and tools would need to be added. With the present definition, all attempted connections at the EAP/ESP would need to be investigated.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Regular reporting to multiple organizations is not cost effective for a small entity. A more cost effective approach might be a "RC" centric approach, where entities must notify Reliability Coordinators, who are regularly responsible for updating appropriate industry entities.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
See comments above.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
APPA believes the drafting team has made an effort to meet directives and be flexible, however, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Requiring the use of a manual form (Attachment 1) for submitting reports does not provide flexibility and will lead to unnecessary administrative costs for E-ISAC, ICS-CERT and the reporting entities. Including a required form as Attachment 1 in the Standard precludes E-ISAC, ICS-CERT and industry stakeholders from collaborating to develop cost effective and timely reporting methods. In order to replace Attachment 1 with a better reporting tool, the Standard would have to be revised in the future which would add additional ERO and stakeholder expense and time delays. As an alternative, please include Attachment 1 within a guidance document as an option for use in the near term.	
Likes 0	
Dislikes 0	
Response	

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	
Tacoma Power agrees with APPA Comments: "APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place.	

Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.

Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report."

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.

Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

Without a clearer definition of attempts, an entity could be overly burdened with administrative and technical tasks associated with investigating, initial reporting and continuous follow-up reporting for insignificant incidents.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Please see the manor of flexabilty of reporting that has a direct correlation to this.

The use of Attachment 1 should not be mandatory because standards should be objective-based and not technology-dependent. Parts 4.2 and 4.4 - Entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information as described in Attachment 1. We appreciate that the SDT confined the requirements for reporting to the three mandatory items identified in the FERC Order.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	

Comment
The proposed changes would take a large number of skilled cybersecurity experts for each RE to investigate and report every attempted Cyber Incident, which adds additional cost without a reduction of risk to the BES. A potential more efficient solution, could be to create an Energy Sector Security Operations Center which aggregates logs from each RE. Creating a Security Opertaions Center, would allow direct reporting to ES-ISAC. It would be more cost effective, provide better metrics with a marco view, allow more flexibility to what FERC wants in the future, and streamline interagency communication processes.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with the following comments submitted by APPA: APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers. Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment
Entities have no technical basis for the classification of attempted incidents and are left with substantial risk and uncertainty with how to implement the requirements and demonstrate compliance using cost effective approaches. Enforcing the proposed modifications in CIP-008-6 as currently drafted could result in inconsistent implementation resulting in fines and penalties.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
Identifying and investigating all potential Reportable Attempted Cyber Security Incidents would be time consuming and costly due to the resources required for these tasks. Additional staffing and tools would need to be added. With the present definition, all attempted connections at the EAP/ESP would need to be investigated.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment
See comments from the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
The additional resources required for data collection, analysis, and reporting could be significant and burdensome, if the proposed criteria for identifying reportable incidents is not revised. Automation seems to be an oversight. The manual process will require hiring additional employees to meet reporting deadlines.

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	

Comment
WAPA agrees that modifications to the standard provide flexibility but WAPA is concerned that there is too much flexibility for interpretation. Auditors and entities will likely **not** agree on the definition of “attempt to compromise.” We suggest further guidance from the SDT. This should be explicitly defined in the requirement and supported with language in the Guidelines and Technical Basis section. We would offer the following examples as a starting point for a more complete list. 1. An “attempt to compromise” could be defined as an act with malicious intent to gain electronic access or to cause harm to the normal operation of a Cyber Asset. a. Actions that are not an attempt to compromise a Cyber Asset electronically include but are not limited to: An entity’s own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent.

Attempts to access a Cyber Asset by user that fails due to human error.

b. Actions that are an attempt to compromise a Cyber Asset electronically include but are not limited to:

Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management. This could be from an entity's own equipment due to an upstream compromise or malware.

Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

2. The word "determination" in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

As drafted, the objectives cannot practically be met in a cost effective manner. For example, Tri-State receives around 912,800 attempts per hour on the business network perimeter firewalls. The drafted language could require Tri-State to report on each of those "attempts" which would dramatically increase personnel and record keeping obligations. Additionally, due to the nature of those we would only be able to provide limited information in reporting, which would likely not be enough information for NERC to achieve their objectives.

However, if the modifications proposed in Comments 1 and 4 were incorporated, this would provide Tri-State with flexibility to meet the reliability objectives in a cost effective manner.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Given thate the new definitions would create big amount of unnecessary reportable cyber security incidents, the compliance management cost will be going up largely. See our comments in question 1.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF agrees the changes to the standard provide flexibility but we are concerned that there is too much flexibility for interpretation. Auditors and entities may not agree on the definition of “attempt to compromise.” We suggest additional guidance from the SDT. This could be in the form of the Guidelines and Technical Basis section or a technical rationale document. We would offer the following examples as a starting point for a more complete list.

An “attempt to compromise” could be defined as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset or a PSP.

Actions that are not an attempt to compromise a Cyber Asset electronically:

An entity’s own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence.

Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent.

Attempts to access a Cyber Asset by user that fails due to human error.

Actions that are an attempt to compromise a Cyber Asset electronically:

Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity’s management. This could be from an entity’s own equipment due to an upstream compromise or malware.

Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

The word “determination” in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	No
Document Name	

Comment
Although the proposed modifications provide flexibility, adding EACMS to the applicable assets can be cost intensive as the Responsible Entity will need to additional resources to review events that maybe determined to be Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment
Given BC Hydro's response and comments to Question #1, BC Hydro does not feel it is appropriate to comment.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	

Comment
I agree the changes to the standard provide flexibility but I am concerned that there is too much flexibility for interpretation. Auditors and entities may not agree on the definition of "attempt to compromise." I suggest additional guidance from the SDT. This could be in the form of the Guidelines and Technical Basis section or a technical rationale document. I would offer the following examples as a starting point for a more complete list. 1. An "attempt to compromise" could be defined as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset or a PSP. a. Actions that are not an attempt to compromise a Cyber Asset electronically: i. An entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence. ii. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent. iii. Attempts to access a Cyber Asset by user that fails due to human error.

b. Actions that are an attempt to compromise a Cyber Asset electronically:

i. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management. This could be from an entity's own equipment due to an upstream compromise or malware.

ii. Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

2. The word "determination" in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

The manner of reporting needs to be flexible. The use of Attachment 1 should not be mandatory because standards should be objective-based and not technology-dependent. Parts 4.2 and 4.4 - Entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information as described in Attachment 1. We appreciate that the SDT confined the requirements for reporting to the three mandatory items identified in the FERC Order.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Dependent on clarification of the term "attempted" as noted in Question 1, implementation of this Standard could be very cost prohibitive.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP recommends providing additional guidance or define attempt. SRP agrees with the attachment form as an industry template for consistency. If reporting attributes change within 5 days adds administration burden of having the template attachment completed. SRP recommends an adjustment to "when the investigation is complete" so an investigation with all the facts are presented. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The current broad nature of the required reporting could lead to excessive burdens in both reporting as well as analyzing the data. Narrowing the definition of an attempt to only impactful attempts would result in a more cost effective Standard.	
Likes 0	
Dislikes 0	
Response	

9. Provide any additional comments for the SDT to consider, if desired.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
See comments of the ISO/RTO Council. Also, ERCOT thanks the SDT for their efforts on this revision.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation recommends Requirement R1 Part 1.1 be changed

from:

One or more processes to identify, classify, and respond to Cyber Security Incidents.

to:

One or more processes to identify, classify, handle, and respond to Cyber Security Incidents.

After the change to Requirement R1 Part 1.1 is made, change the measure in Requirement R1 Part 1.1

from:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

to:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, handle, and respond to Cyber Security Incidents (e.g., containment, eradication, recovery/incident resolution).

When the change to Requirement R1 Part 1.1 measure is incorporated, remove Requirement R1 Part 1.4.

Reclamation also recommends changing the timeframe specified in Requirement R3 Part 3.2 to 90 days to align with the time allowed in Requirement R3 Part 3.1.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment

AECI supports the comments provided by NRECA.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	
Document Name	

Comment

In Parts 4.3 and 4.4, Dominion Energy recommends clarifying that the determination is the entity's determination for the 5 day clock to begin.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	
Comment	
It is unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a network. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond network noise.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP recommends providing additional guidance or define attempt. Reporting if attributes change within 5 days will add administration burden of having the template attachment completed. SRP recommends an adjustment to when the investigation is complete so a complete investigation with all the facts are presented in the template attachment. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	
Document Name	
Comment	
The new/updated standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	

Answer	
Document Name	
Comment	
The new/updated standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	
Document Name	
Comment	
The new/updated Standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
The addition of EACMS functions creates a second definition of the term. If the five functions are what the SDT considers an EACMS to fulfill, the official definition should be modified to include these to avoid differing interpretations of the term based on the Standard.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	
Document Name	

Comment
Change terms to add “Successful” to Reportable “Successful” Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both “Reportable” terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding “Successful” to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove “and requires notification per Requirement R4.” This is redundant with R4. According to the NERC webinar, the SDT’s intent was to remove “notification” from part 1.2 One stop approach – change Requirement 4 to require Registered Entities submit the Attachment 1 content to E-ISAC only. E-ISAC would anonymize it, submit it to ICS-CERT and forward a copy of the submission to the reporting entity as evidence. This preserves confidentiality, simplifies reporting and provides evidence. If Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents must be reported separately to DHS’s ICS-CERT, what does NERC and the SDT propose to do to preserve confidentiality and to protect BES reliability from disclosed infrastructure information when DHS is subject to the Freedom of Information Act? For Requirement part 4.1, remove “Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,.” This requirement is about defining the content of the report, not defining which scenarios are reportable. If Attachment 1 is mandatory and “unknown” is the only acceptable response when an attribute hasn’t been identified yet, please add an “Unknown” checkbox to make it easier for entities who are dealing with an incident. References to “Click or tap here to enter text.” are out of place because they are not functional and shouldn’t be there. It creates confusion. Attachment 2 Functional Impact examples should reference the reliability tasks referenced in the NERC Functional Model. See footnote 19 on page 13 of the FERC order.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1	
Answer	
Document Name	

Comment
The proposed standard has the potential to create a significant auditing burden regarding “attempts to compromise,” which have no impact on reliability. 1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives. 2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro requests explicit clarity on whether Physical Security Perimeter breaches alone without any established breach or compromise of any BES Cyber Systems, ESPs, or EACMS would be considered a potential Reportable Cyber Security Incident. On the NERC led webinar on the CIP-008-6 proposed revisions of October 16, 2018, it was communicated that PSP breaches alone would not constitute a Reportable Cyber Security Incident, however, Requirement 4.1 as written, implies that PSP breaches would constitute potential Reportable Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	
Document Name	

Comment

When an event is determined to be a Cyber Security Incident, the Responsible Entitiy needs to determine if it is a Reportable Cyber Security Incident or a Reportable Attempted Cyber Security Incident. The SDT should consider retiring the term Cyber Security Incident. The modified Reportable Cyber Security Incident and the proposed Reportable Attempted Cyber Security Incident definitions provide the identification and required notifications required for the implementation of CIP-008-6.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The proposed standard has the potential to create a significant auditing burden regarding “attempts to compromise,” which have no impact on reliability.

1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives.

2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	

WEC Energy Group is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. WEC Energy Group recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

While WEC Energy Group recognizes that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

An additional area where we'd like to see further clarification is related to the definition of Cyber Security Incident. It includes compromise or attempt to compromise (2) Physical Security Perimeter, yet PSPs aren't mentioned anywhere else in the standard except to be explicitly excluded in Requirement R4 part 4.1. We assume the linkage is to CIP-006 Requirement R1.5 and R1.7 which require generation of an alert to Cyber Security Incident Response personnel in the event of detected unauthorized physical access to PSP or PACS. We would like the SDT to spend more time on building and explaining the linkage, especially since CIP-006 only requires alert of an actual breach and the proposed CIP-008 requires notification of breach attempts. Also, rationale for the exception in R4 part 4.1 would be helpful.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

1. It is difficult to determine attempts of compromise and SDT should clarify what constitutes an "attempt of compromise". Otherwise, registered entities may have different interpretations resulting in the consistency issue.

2. The timeline statement in Part 4.2 should be moved to Part 4.3 since the Part 4.2 only addresses the notification methods. Also given that the wording "responsible entities "never appears in the Parts, we suggest to remove "responsible entities " from Part 4.2 and reword Part 4.2 as follows:

"One of the following methods for initial notification shall be used:

• Electronic submission of Attachment 1;

• Phone; or

• Email. "

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment

Regarding Definitions and Reporting: For clarity on current-state reporting and direction for future unforeseen technology and methods, it would be helpful if SDT could provide a list of examples of what would be considered a Reportable Cyber Security Incident versus an Attempt. The list would not

need to be all-inclusive of any potential threats, but would help with consistency and questions. For example, is phishing considered an attempt? The list could be similar in format and methodology to EOP-004 Emergency Preparedness and Operations: Event Reporting.

Regarding R4 and Attachment 1: In order to effectuate recordkeeping, we suggest that after reporting has been submitted, the entity receives a confirmation with a case number. In the event of future updates, the case number can be referenced to locate the records referenced and update the corresponding information. This will also serve as a method to align recordkeeping and maintain evidence that submissions have been received. Alternatively, and at a minimum, the reporting form should include some type of identifier that can be cross-referenced across updates, like a date field (date of the incident, date it was identified, date it was originally reported, etc.)

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

It would be useful if the implementation plan included several examples of instances where the SDT believe are reportable attemps to compromise or disrupt the Electronic Access Control of Monitoring System or the operations of a BES Cyber System. Seattle City Light believes the possible interpretation could be overly broad.

It was discussed on the SDT webinar that “anything out of the normal range of activity” should be considered an attempt. The example being discussed was IP address scanning. One utility might receive random scans 10 times a day on average to a certain address and an other might experience 100 on average. A brighter line defining an attempt and/or examples would be helpful.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

We suggest changing the language in “CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents” so that the wording is consistent throughout its contents. Parts 4.2 and 4.4 use the terminology “Responsible Entities shall use…” in the “Requirements” column, whereas Parts 4.1 and 4.3 do not, nor do other standard requirements.

Likes 0	

Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	
Document Name	

Comment

The proposed standard has the potential to create a significant burden on entities regarding “attempts to compromise,” which have no impact on reliability and will hinder the entities ability to respond to real cyber incidents. The potential increase in investigation and reporting of incidents could lead to a major compromise by allowing bad actors to feint attacks in one area to distract while simultaneously attacking in another area.

WAPA agrees with NSRFs additional comments and includes them with our own.

1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives.

2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

ALSO: Reclamation recommends the SDT provide clarifying information to distinguish between the requirements of R1 Part 1.1 and Part 1.4.

Therefore, Reclamation recommends Requirement R1 Part 1.1 be changed

From One or more processes to identify, classify, and respond to Cyber Security Incidents.

to

One or more processes to:

· Identify and classify Cyber Security Incidents.

· Describe handling procedures related to Cyber Security Incidents.

When this change is incorporated, Reclamation also recommends removing requirement 1.4.

Reclamation also recommends specifying that records related to Requirement R2 Part 2.3 be maintained for 15 months following the initial date of reporting the incident to the E-ISAC.

Reclamation also recommends the timeframes specified in Requirement 3 Part 3.2 coincide with the 90 days specified in Requirement R3 Part 3.1, rather than 60 days.

Reclamation also recommends Requirement 4 not include a mandate for entities to notify the ISC-CERT. Replace “ISC-CERT” with the “U.S. Department of Homeland Security” instead of any specific CERT entity within US DHS.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	
Document Name	
Comment	
Our SMEs believe that responding to an attempted reportable incident should be included as way to test your plan once every 15 months in CIP-008-6 Table R2 2.1.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Where will reported data be stored? How will the data be protected? Who will be liable for a data breach at E-ISAC or ICS-Cert? Entities will have to spend much time and money to recover from a data breach and to re-secure critical systems.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	
Document Name	

Comment
While we believe this is a well-thought out modification to CIP-008, we still have concerns regarding the possibility of under or over-reporting as compared to our peers and whether or not being outside of the normal reporting frequency (or bell curve) will create additional scrutiny from regulators. While there is supposed to be a barrier between E-ISAC/ICS-CERT and auditing entities, NERC and the SDT should consider how this separation will be enforced to reduce undue scrutiny for Responsible Entities (REs) who may have varying interpretations of what should and should not be reported. Ensuring clear Implementation Guidance may address this concern. The modification to R1.2 now includes a cross-reference to R4, which adds complexity to interpretation. We recommend this be a separate sub-requirement or otherwise tied in to R4. We noted that the main verbiage in Requirement 4 is structured differently than other CIP requirements which generally instruct REs to implement a plan or process with more specific details included in a sub-part. That information (who to notify) should instead be incorporated into a sub-part for consistency. We are also concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. We recommend clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliability Standard. While we recognize that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment
The Guidelines and Technical Basis in CIP-008-6 Draft 1 references a technical rationale document, but this has not been posted. While a technical rationale is not enforceable and cannot change the language of the Standard, it can provide a context within which the understanding of the Standard may change. This document needs to be posted for public review before comments on the revised language of CIP-008-6 Draft 1 will be meaningful. CIP-008-6 R1 Part 1.2 requires the Incident Response Plan to include processes to determine whether an incident is reportable, but does not require a documented process for notification. R4 does not require such a process either. However, the Measures for Part 1.2 reference “documented processes for notification.” If the SDT intends that a process for notification be included in Part 1.2, this should be clearly stated in the Requirement language. CIP-008-6 R4 Part 4.3’s Requirement section contains a parameter, not a Requirement. Suggested wording is, “Responsible Entities shall submit initial notification in accordance with the following timeline: …” The first sentence of the Requirement for CIP-008-6 R4 Part 4.4 requires submission of Attachment 1 updates for new or changed information. The second sentence only requires submissions for new attribute information until all attributes have been reported. The second sentence is contradictory and superfluous to the first sentence and should be deleted.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends adding Attempted Reportable Cyber Security Incident to Requirement Parts 3.1 and 3.2 to be consistent with Requirement Part 2.2. If the Cyber Security Incident Response Plan(s) is to be used when responding to an Attempted Reportable Cyber Security Incident (Part 2.2), the plan should also be reviewed and updated after responding (Parts 3.1 and 3.2). With the addition of the definition of Reportable Attempted Cyber Security Incident, Texas RE inquires as to whether that should be included in Requirement Part 2.1. Is a Reportable Attempted Cyber Security Incident considered a test of the entity's plan?	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA believes it's unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
Utility Services thinks that the not including "disrupt" in the definition of a Cyber Security Incident in the same way as it is included in the Reportable Cyber Security Incident definition leaves the difference between "compromised" and "disrupted" open to interpretation. We poses that entity definitions for "compromise" and "disrupt" should be included in the same way "programmable" is. In R4, we are concerned with the phrase "or their successors", which could lead to required reporting to all companies or agencies that make a claim to be successors to either E-ISAC or ICS-CERT. If ICS-CERT changes its name, it is still ICS-CERT. If needed, CIP-008 could be revised to reflect the name change in its next update. In M4, Utility Services is concerned that Reportable Attempted Cyber Security Incident is not included, only Reportable Cyber Security Incident. Since R4 includes Reportable Attempted Cyber Security Incident , consistency would be better maintained if M4 included the term as well. On a different note, the word “determined” within M4’s language seems superfluous since R1.2 uses “determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident ”. We think the fact that, in R4.1, the exclusion of Physical Security Perimeter is confusing since the definition of Cyber Security Incident includes Physical Security Perimeter but Reportable Cyber Security Incident does not. By this, a Cyber Security Incident including a compromise to a Physical Security Perimeter **and** Electronic Security Perimeter would not need to be reported since it includes a Physical Security Perimeter. Additionally, in order to maintain consistency with Attachment 1 and R4.2, we propose changing “attributes” to “attribute information”.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	

Comment
We believe it’s unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	

Comment

No comment	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	
Document Name	
Comment	
GSOC believes it’s unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	

E ISAC and ICS-CERT should provide incident reporting / information sharing portals for use by Responsible Entities that meet notification and attribute submittal requirements in the proposed CIP 008-6 modifications.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	
Document Name	

Comment

Reporting should be simplified, such as the IP address and service or port that was blocked, and sent periodically (monthly or quarterly) for use by E-ISAC and/or ICS-CERT for correlation across the industry. This simplified reporting would greatly reduce the burden on the entity and still provide the reporting and data necessary to meet the intent of FERC Order No. 848.

Vectren is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. Vectren recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you for allowing Vectren the opportunity to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CenterPoint Energy understands the objectives of the modifications and their alignment with the FERC directives. However, the concept of “Reportable Attempted Cyber Security Incident” is nebulous. There are past unsuccessful deliberations from attempting to require responsible entities to determine intent as in the efforts to define and enforce “Sabotage Reporting.” The definitions and Requirement 4 have inconsistencies and concepts still to be interpreted. The result of these modifications could be more reporting with little value.

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	
Document Name	
Comment	
Attempts to compromise connected systems happen thousands of times every second of every day. They are typically scripted, spoofed, and performed by BOTNETs. BOTNETs can create thousands of attempts per second. Reporting these would be impossible and create significant burden on the RE and NERC. Thank you for allowing us to comment.	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	
Document Name	Revisions to R4.docx
Comment	
AZPS recommends the change to R4 shown in the attached for clarity.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the	

information reported public. EEI recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

While EEI recognizes that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

ATC appreciates the SDT's thoughtful approach to minimize, to the extent possible, modifications to existing language and the mindfulness of unintended consequences. ATC requests that the SDT continue to focus on what, and not how to prevent CIP-008 from becoming overly prescriptive.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment
Part 1.2 – Remove: '…and requires notification per R4.4' = redundant. You removed the 1 hour requirement in R1.2. Same things on the measures too. *Section 215 INCLUDES PSP – NERC should not start to EXCLUDE it. Recommend striking the following statement from the language: "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter," out of the language of the requirement. Add a check box in the three fields for attributes, of "unknown" until all attributes have due to the term, "without attributes The 'click or tap…' section is not listed in all three sections, as well as, it is not functional – suggest remove or repair. Change terms to add "Successful" to Reportable "Successful" Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both "Reportable" terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding "Successful" to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove "and requires notification per Requirement R4." This is redundant with R4. According to the NERC webinar, the SDT's intent was to remove "notification" from part 1.2. reporting to the three mandatory items identified in the FERC Order. {C}1. Provide any additional comments for the SDT to consider, if desired. Comments: Part 1.2 – Remove: '…and requires notification per R4.4' = redundant. You removed the 1 hour requirement in R1.2. Same things on the measures too. *Section 215 INCLUDES PSP – NERC should not start to EXCLUDE it. Recommend striking the following statement from the language: "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter," out of the language of the requirement. Add a check box in the three fields for attributes, of "unknown" until all attributes have due to the term, "without attributes The 'click or tap…' section is not listed in all three sections, as well as, it is not functional – suggest remove or repair. Change terms to add "Successful" to Reportable "Successful" Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both "Reportable" terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding "Successful" to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove "and requires notification per Requirement R4." This is redundant with R4. According to the NERC webinar, the SDT's intent was to remove "notification" from part 1.2 **One stop approach** – change Requirement 4 to require Registered Entities **submit** the Attachment 1 content **to E-ISAC only**. E-ISAC would anonymize it, submit it to ICS-CERT and forward a copy of the submission to the reporting entity as evidence. This preserves confidentiality, simplifies

reporting and provides evidence. If Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents must be reported separately to DHS's ICS-CERT, what does NERC and the SDT propose to do to preserve confidentiality and to protect BES reliability from disclosed infrastructure information when DHS is subject to the Freedom of Information Act?

For Requirement part 4.1, remove "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,." This requirement is about defining the content of the report, not defining which scenarios are reportable.

If Attachment 1 is mandatory and "unknown" is the only acceptable response when an attribute hasn't been identified yet, please add an "Unknown" checkbox to make it easier for entities who are dealing with an incident. References to "Click or tap here to enter text." are out of place because they are not functional and shouldn't be there. It creates confusion. Attachment 2 Functional Impact examples should reference the reliability tasks referenced in the NERC Functional Model. See footnote 19 on page 13 of the FERC order.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	
Document Name	

Comment

We appreciate the hard work of this standard drafting team and the extra burden placed on the team by the accelerated timeline. Our comments are intended to support the team in providing the best solution to this issue with a balance between focusing on a response to the immediate threat, providing timely notification to the appropriate agencies, and addressing the concern of an unwarranted breach of confidential information. - Vistra Energy / Luminant

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

E ISAC and ICS-CERT should provide incident reporting / information sharing portals for use by Responsible Entities that meet notification and attribute submittal requirements in the proposed CIP 008-6 modifications.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	
Document Name	

Comment

Single-Point of Data Reporting

The companies are aware of the SDT's discussions and the industry's input regarding: E-ISAC acting as a single point of data acceptance, and E-ISAC forwarding the data to ICS-CERT.

We also have listened to the industry's appeal for an electronic method to submit the required data—an idea that we support. Nevertheless, the companies also recognize there is a limitation of FERC not having regulatory authority to require E-ISAC develop and accept the data through an electronic portal, nor ICS-CERT, for that matter.

With that being the case, and beyond the likely efficiency offered by single-point of data reporting, we have identified a specific concern we believe weakens the proposed CIP-008 revisions; specifically, in the event an electronic, single point of reporting is unavailable to the industry, the proposed CIP-008 revisions will require reallocation of scarce cyber security personnel resources from high-value analysis, monitoring, mitigation, and protection activities to manage inefficient data reporting.

With the potential to weaken security because of reassignment of personnel, we highlight our concern and encourage the SDT to continue its efforts to bring E-ISAC and ICS-CERT into the data submission and reporting methodology discussion.

(Note: "Scarce cyber security personnel resources" refers to the limited pool of available professionals to fill cyber security positions; it is not necessarily a question of expanding cyber security staffs but the competition between all industries to hire trained, experienced, cyber security professionals that can pass background checks.)

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

The information protections that DHS ICS-CERT would use for handling incidents reported to them is not clear and causes concern for APPA. It remains unclear whether the reports submitted to DHS will be subject to Freedom of Information Act (FOIA) requests or whether DHS will consider the

reports public information. APPA believes NERC needs to understand how DHS will classify the data and what confidentiality provisions will be in place, prior to making this an enforceable standard.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	
NCPA is in agreement with APPA and USI's comments. Thank you.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
Measure 4 and Requirement R4.1 imply but appear to be missing the insertion of the term “Reportable Attempted Cyber Security Incident”	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
The SDT should consider whether adding CIP Exceptional Circumstances to CIP-008 reporting would make sense given some incidents may make reporting difficult for the timelines currently under consideration.	

4.3 High Impact BES Cyber Systems and their associated:

· EACMS

Medium Impact BES Cyber Systems and their associated:

· EACMS

Except when operating under CIP Exceptional Circumstances, theTimeline for initial notification will be:

· One hour from the determination of a Reportable Cyber Security Incident.

· By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.

Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of phone records for preliminary notice or submissions through the E-ISAC and ICS-CERT approved methods, or Attachment 1 submissions.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	
Document Name	

Comment

Like many of our peers, Exelon has concerns regarding the standard not officially defining “attempts”. The drafting team should define parameters where its apparent certain controls have been misused, for example, if authentication credentials were compromised. As well, the drafting team could modify the language to instruct organizations to develop a program or process based on their unqiue characteristics for determining or classifying what the entity classifies an attempt.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	
Document Name	

Comment

Agree with the comments made by Lynn Goldstein for PNMR.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

Ensure references to "Version 5 CIP Cyber Security Standards" is updated similar to changes made in CIP-002-6.

Recommend the SDT consider adding Physical Security Perimeter or Physical Access Control Systems (PACS) into the applicable systems for CIP-008-6 to ensure any attempts, successful or unsuccessful to compromise the responsible entities PSP or associated PACS are obtained to gain a better understanding of the full scope of cyber-related threats facing the Bulk-Electric Power System(s).

Disagree that Part 4.1 shoulde exclude incidents involving PSPs. The listed items could be applicable to a compromise of a PSP and such incidents should be considered applicable to the entirety of R4.

In Attachment 2 for “Reporting Category” – “Update” field, the reference is to Part 4.2 but appears to be incorrect and should perhaps reference Part 4.4 instead.

As it relates to the SDT not updating the Guidelines & Technical Basis narrative to reflect the changes in CIP-008-6 due to the Technical Ratinale project, it should be considered for removal or updates should be made accordingly. These sections are frequently used by industry and failing to update them could lead to greater confusion.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	
Document Name	

Comment

Reporting should be simplified, such as the IP address and service or port that was blocked, and sent periodically (monthly or quarterly) for use by E-ISAC and/or ICS-CERT for correlation across the industry. This simplified reporting would greatly reduce the burden on the entity and still provide the reporting and data necessary to meet the intent of FERC Order No. 848.

Vectren is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the

information reported public. Vectren recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you for allowing Vectren the opportunity to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

In R4, Southern Company is unclear as to the meaning of “United States Responsible Entity.” Does this refer to where an entity is headquartered, or does it refer to the location of the affected cyber systems? Additional clarification regarding the intent of this statement is requested in future revisions of the draft.

Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Southern Company is opposed to the SDT addressing the “How” in the Standard. The requirements should dictate “What” information is required to be provided, and to whom, but not “How” entities provide it. Examples of “How” should be deferred to implementation guidance, not imposed as requirements within the Standard.

Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-6

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting: Consideration of Comments

November 2018

RELIABILITY | ACCOUNTABILITY



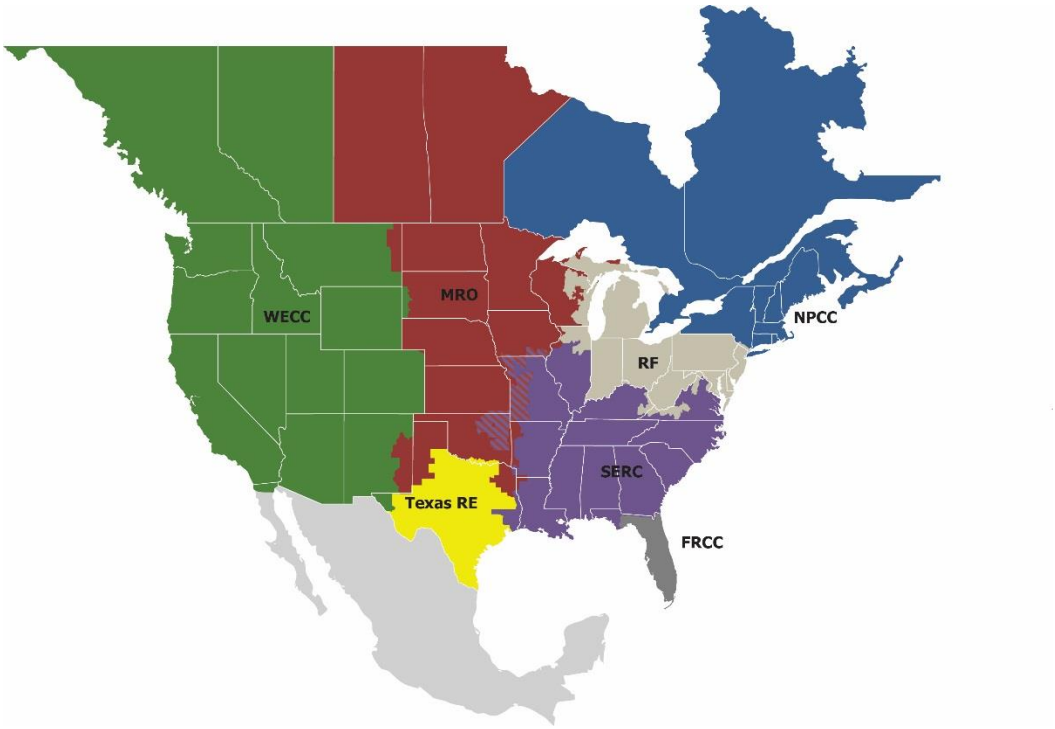

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven regional entities (REs), is a highly reliable and secure North American Bulk-Power System (BPS). Our mission is to ensure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries, as shown below in the map and corresponding table. The downward diagonal, multicolored area denotes overlap because some Load-Serving Entities participate in one region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team thanks all commenters who submitted comments on the draft CIP-008-6 standard. This standard was posted for a 20-day public comment period, ending Monday, October 22, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 86 sets of responses, including comments from approximately 176 different people from approximately 116 companies, representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Alison Oswald, at 404-446-9668 or at alison.oswald@nerc.net.

CIP-008-6 Consideration of Comments – Summary Responses

Purpose

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team (SDT) appreciates industry's comments on the CIP-008-6 standard. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and the SDT's corresponding responses. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Definitions

Several commenters asked for clarity in the definitions for attempts to compromise, how BES Cyber Assets (BCAs) are included, and the potential for having only one definition.

The SDT made changes to the requirements to clarify that the Responsible Entity determines attempt to compromise through their processes for reporting. Verbiage has been added to CIP-008 R4, Part 4.2 that links the process to determine reportability defined in CIP-008 R1, Part 1.2 to the obligation to report after the determination is made by the Responsible Entity.

The SDT addressed BCAs by adding BCS to the Reportable Cyber Security Incident definition. The team asserts that the modification aligns with the intention of FERC Order 848 Paragraph 52 that describes BES Cyber Systems within the ESP.

The SDT also reviewed the comments that addressed consolidating the definitions into one definition. The team made the decision to remove the proposed Reportable Attempted Cyber Security Incident definition. Instead, CIP-008 R4, Part 4.2 has been updated to include conditions for reporting Cyber Security Incidents that only attempt to compromise a system identified in the "Applicable Systems" column for this part. The modification does not impact the definitions of Cyber Security Incidents and Reportable Cyber Security Incidents that exist in both CIP-008 and CIP-003, and eliminates the need for a standalone definition for Reportable Attempted Cyber Security Incidents.

Attachment 1

Many commenters expressed concern with requiring reporting to occur in the format of Attachment 1.

Based on comments received and consultation with representatives from the Electricity Information and Analysis Center (E-ISAC) and the National Cybersecurity Communications Integration Center (NCCIC), which is the successor organization to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the standard has been updated such that Attachment 1, and the supporting instructions called Attachment 2 have been removed from the standard and are no longer required. The form and instructions have been moved to draft Implementation Guidance as an option for Responsible Entities to use at their discretion.

Many commenters expressed concern with the methods of submitting the three required attributes being prescriptive and disagree with updates having to be submitted in only Attachment 1 form.

The SDT determined it was not necessary to define the method for notification, and the initial proposed Requirement R4, Part 4.2 has been removed. Attachment 1 is no longer required, and has been moved into the draft Implementation Guidance.

Some commenters mentioned that the new form should fit with other forms and existing reporting requirements to avoid duplication (utilize EOP-004-4 and/or Department of Energy's OE-417)

The SDT has removed the proposed requirement for utilizing the proposed Attachment 1. However, the SDT determined not to modify existing reporting forms, such as OE-417, because Order No. 848 noted that this form did not request information that FERC directed the SDT to require in CIP-008. Nonetheless the SDT notes that entities

may consider synchronizing their reporting processes as long as all information that is required to be reported is submitted to appropriate agencies.

Some commenters would like to leverage reporting to a single agency as an intermediary to the other agency.
The SDT thanks you for your comment, however the SDT asserts that the proposed reliability standard is responsive to FERC Order 848 and that this is outside of the scope of the SAR.

Information Protection

One initial point of clarification: ICS-CERT functions are now handled by the Department of Homeland Security (DHS) National Cybersecurity and Communication Integration Center (NCCIC) and incident reports will be submitted through existing NCCIC incident reporting mechanism rather than anything specific to ICS-CERT. Any future references will be to NCCIC, which is ICS-CERT's successor organization.

Many commenters expressed concern over information protection once information is submitted to E-ISAC and NCCIC.
During the meeting the SDT submitted these concerns to both the E-ISAC and NCCIC. Both organizations assured the SDT that they have multiple ways to secure information that is submitted. Options include:

- Utilizing a secure/encrypted portal; or
- Encrypted e-mail (via Pretty Good Privacy – PGP)

Please note the following answers are directly from DHS.
Many commenters expressed concern if DHS will make the information reported public.
DHS will not attribute any information back to an entity but may incorporate the non-attributable and anonymized information into publicly available products to enable stronger cybersecurity protections and response activities for similarly situated entities. Such use or incorporation will only be done without attribution to the original entity and with the removal of any contextual information that could enable an entity's identification, unless the entity expressly agrees otherwise in writing.

Many commenters expressed concern about what confidentiality provisions will be in place for information submitted to DHS.
DHS will not attribute any information back to an entity and will use cover names for the entity within the NCCIC to protect the entity's identity. Information submitted through email can be done so with the DHS PGP key to keep information confidential. In addition, the web-based portal has security in place to protect information submitted through that option.

Many commenters wanted assurances that phone conversations with DHS are confidential.
Submissions by phone are added to the incident management system as tickets and are entitled to the same protections as submissions provided through email or web form.

Many commenters expressed concern over where reported data will be stored at DHS.
Data will be handled and stored with other sensitive incident reporting data the NCCIC receives and triages from various public and private sector entities.

Many commenters asked who will be liable for a data breach at NCCIC.
DHS has no comment regarding this issue.

Many commenters expressed concern that the reports submitted to DHS will be subject to Freedom of Information Act (FOIA) requests.

DHS has successfully exempted similar information from FOIA in the past under various FOIA exemptions defined at 5 U.S.C. § 552(b), to include Exemption (b)(3) as specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial information that is privileged or confidential, and Exemption (b)(7)(A)-(F) as records or information compiled for law enforcement purposes. To the extent incident reports contain cyber threat indicators and defensive measures that meet the definition of cyber threat indicator or defensive measure as defined in the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501-1510 ("CISA"), and that is provided in accordance with CISA's requirements, such information will be protected as provided by CISA (including protection from release under FOIA). See the Non-Federal Entity CISA Sharing Guidance published by the Department of Homeland Security and the Department of Justice, available at https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

Many commenters inquired if entities will receive confirmation receipt or other methods to ensure DHS received information.
DHS will provide entities with a ticket number upon receipt of information.

Notification Approach

Many commenters suggested increasing the initial notification timeframe for attempts to compromise (which was defined in the first proposed draft as a Reportable Attempted Cyber Security Incident) from the next calendar day to the next business day.
The SDT asserts the end of the next calendar day is sufficient time for notification. The preliminary notification is not triggered until a Responsible Entity has made a determination on classification of reportability and does not require all of the attributes to be identified if undetermined at the time of notification. The determination defines the start time for reporting. Business day is a difficult term to define, particularly in 24x7 business environments. However, the SDT asserts that the end of a calendar day is understood to be 11:59pm local time.

Some commenters suggested increasing the initial notification timeframe for Reportable Cyber Security Incident from 1 hour to 2 hours.
FERC Order No. 848 instructs the SDT to consider risk when developing timeframes. The SDT asserts that the 1 hour timeline is in alignment with previous versions of CIP-008, other FERC orders, and severity of the incident. This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable. It does require preliminary notification, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report. The SDT also asserts that means exist to provide simultaneous notification. The time required to notify additional entities does not begin until the entity has made a determination that aligns with a reportable classification.

Many commenters suggested increasing the timeframe for updates to the three required attributes to within 7 days instead of 5 days.
The SDT has adopted this recommendation.

Many commenters expressed confusion that initial notification and updates are not required until an incident is "determined" by an entity to be reportable or reportable attempted.
The SDT has added clarifying language in Requirement R4, Part 4.2 that refers to Requirement R1, Part 1.2, where Responsible Entities define their process(es) for determination of reportability.

Attempts

Several commenters expressed concern about the determination of "attempts" and requested the SDT either define "attempts" or provide clear examples within Implementation Guidance to aid the industry.

The SDT asserts that it is to the industry's benefit that CIP-008 leaves it up to each Responsible Entity to document a process to determine what constitutes an "attempt". The SDT further asserts that no two Responsible Entities are alike and the determination of "attempts" is contextual and dependent on what is normal within each unique organization. To define "attempt" could create an overly prescriptive and less risk-based approach and may have the unintended consequence of undue administrative burden or removal of needed discretion and professional judgment from subject matter experts. The SDT has developed proposed Implementation Guidance inclusive of several examples in an effort to address this issue.

Some commenters suggested monthly reporting for minimal risk attempts to the ERO and questioned the value of proposed reporting timeframes.
Thank you for your comment. The SDT asserts that the reporting timeline for attempts to compromise is in alignment with FERC Order No. 848 and is in the spirit of timely reporting for information sharing.

PSPs

Commenters expressed confusion on how the standard relates to Physical Security Perimeters (PSP) and in some instances requested the removal of PSP from the Cyber Security Incident definition.
Regarding PSPs, the currently enforceable definition of Cyber Security Incident includes malicious acts or suspicious events that compromise, or attempt to compromise, PSPs. The currently-enforceable Reportable Cyber Security Incident definition includes Cyber Security Incidents that have compromised or disrupted one or more reliability tasks of a functional entity. As such, compromises or attempts to compromise PSPs could be reportable under the currently enforceable standard and definition. The SDT understands the concern but determined not to lessen the reporting obligation from that of the currently enforceable standard. In addition, the SDT reviewed the directives from FERC Order No. 706 that directed NERC to take into account in CIP-008 a breach that may occur through cyber or physical means. As a result, the SDT will not remove PSP from Cyber Security Incident. As an example, this issue is also addressed in CIP-006-6, Requirement R1, Part 1.5, among others, where Responsible Entities must issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

Some commenters wanted to understand the omission of Physical Access Control Systems in the Applicable Systems column of the standard.
The SDT asserts the modifications proposed are in response to FERC Order No. 848.

EACMS

Multiple commenters were concerned that the inclusion of the five functions modified the definition of Electronic Access or Monitoring Control Systems (EAMCS) and either narrowed or broadened the scope of that definition.
The SDT considered comments regarding the inclusion of the five EACMS functions within the proposed revised definition for Reportable Cyber Security Incidents and what had been a new proposed definition for Reportable Attempted Cyber Security Incidents in the first draft. The industry was divided on this subject in that some entities view the inclusion of these functions as an attempt to modify or expand the scope of the existing EACMS definition and want it stricken, while others view the inclusion as a limiting factor and prefer to retain the language in the definitions. *The SDT concluded that neither the inclusion nor exclusion affects the current definition of EACMS.*

The SDT asserts that the inclusion of these five functions within this proposed definition is unnecessary and not appropriate at this time. The SDT discussed at length both sides of the issue and decided to remove the five functions for the following reasons:

1. The team has adjusted the definition of Reportable Cyber Security Incident and the Applicable Systems column and requirement language for attempts to compromise to align directly with the FERC Order

Paragraph 54 and believes these five functions are the essence of an EACMS by the current definition and to restate them is redundant.

2. The inclusion of these functions may create a new sub-classification EACMS resulting in potential confusion and undue administrative burden for Responsible Entities to establish and implement new processes to reclassify. This may unnecessarily complicate, create confusion, or introduce delay in timely information sharing.
3. Regional inconsistencies with interpretation should be referred to NERC staff for evaluation of and submission through the alignment tool. NERC Project 2016-02 is also in the process of modifications to the NERC Glossary of Terms definitions for Interactive Remote Access, Intermediate Systems, and Electronic Access Control or Monitoring Systems. Additionally, the Project 2018-02 SDT has decided not to modify these terms due to their pervasive use throughout CIP Reliability Standards and the abbreviated timeline for filing of CIP-008-6 as directed in FERC Order No. 848.
4. In addition, while the SDT understands the potential for opposing interpretation, the use of the words "at a minimum" in FERC Order No. 848 Paragraph 54 suggest an intention to limit scope, which the SDT will address within Technical Rationale and Interpretation Guidance.

The SDT reevaluated FERC Order No. 848 and asserts that these five functions align with the directive in Paragraph 54 and are also are consistent with the EACMS definition. By definition, EACMS are, "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems. This includes Intermediate Systems." When analyzing these five functions against this definition, the SDT determined each function is traceable to a component of the EACMS definition. The following list is a mapping of the five EACMS functions from the FERC directive to the current enforceable definition in demonstration of this alignment.

An EACMS associated to a High or Medium impact-rated BES Cyber System (H/M BCS):

(1) performing an **authentication** function, constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems;
(2) performing a **monitoring and logging** function constitutes a Cyber Asset that performs electronic access monitoring of the ESP or BES Cyber Systems;
(3) performing an **access control** function constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems;
(4) performing an **Interactive Remote Access** function constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems; and
(5) performing an **alerting** function constitutes a Cyber Asset that performs electronic access monitoring of the ESP or BES Cyber Systems.

Some commenters asked that the five functions be put in the Applicable Systems column or the requirement language.
The SDT concluded that neither the inclusion nor exclusion affect the current definition of EACMS and chose not to include the five functions in the Applicable Systems column. Please see justification above to support this decision.

Some commenters asked the SDT to modify the EACMS definition.
The SDT evaluated the potential impact and unintended consequences due to its pervasive use throughout the standards and elected not to modify the EACMS definition.

Commenters were concerned that adding EACMS to the Applicable Systems column was pulling in new monitoring or alerting systems and creating a "hall of mirrors."
The SDT is not modifying the existing definition of EACMS. Adding EACMS to the Applicable Systems column does not change which Cyber Assets are classified under the currently-enforceable standard as EACMS.

Commenters suggested EACMS does not need to be in the definition if it is in the Applicable Systems column.
The SDT asserts that the presence of EACMS in the Reportable Cyber Security Incident definition and the Applicable Systems column provides clarity and aligns with FERC Order No. 848 to expand reporting to EACMS.

Implementation Plan

Multiple commenters stated a 12-month implementation phase is not sufficient to accommodate the increased workload associated with increased reporting requirements.
The SDT considered comments related to the amount of time needed for successful implementation of the modifications to CIP-008 (Project 2018-02) and agrees with the need for additional time to make the necessary adjustments. Consequently, the SDT assert that an 18-month implementation timeline is necessary and appropriate for the reasons provided below.

Impact on Small Business Entities
The FERC Directive (Order No. 848) was intended "to result in a measured broadening of the existing reporting requirement" in CIP-008-5, and not create a "wholesale change in cyber incident reporting".1 While this may be true for larger electric utilities, the SDT considered the impact of increased reporting requirements on all NERC-regulated entities and has determined that small-business entities – those with a limited customer base, lower annual revenue/mile of transmission line, and located in rural areas – have fewer resources available to meet increasingly granular requirements, as well as zero-consequence incidents.

Small entities are more susceptible to problems in hiring a number of problems in hiring and retaining cybersecurity staff, including competitive salary, progressive career path, retiring employees, and smaller applicant pools. Lack of trained staff results in increased costs for consulting services for system design and architecture, professional engineering, network design and integration, and technical support. The budget request process to secure consulting services, as well as the resulting recommendations for equipment, requires preparation and justification, and appropriate time is needed.

While the Commission states that entities are already required to perform system security monitoring (CIP-007 Requirement R4), there are certain considerations for smaller entities that may have been overlooked. The difference between logging events (per BES Cyber System or Cyber Asset capability) and reviewing the logged events is significant. Smaller entities may have older equipment (decreased capabilities) and lower-impact BES Cyber Systems (not high-impact which requires review/sampling of logged events) and the new requirements create an increased need for securing additional resources (including trained professionals). For many entities, including not-for-profits, budget approval cycles may exceed 12 months, and the timing of the effective date may make the requirement difficult to achieve for these entities.

New or modified compliance documentation
All NERC-registered entities will bear the burden of developing updated documentation necessary to prove that specific actions, processes, and standards are met, vetted, and approved. The documentation may include updated roles and responsibility matrices, flowcharts, development and implementation of internal controls,

[1] 2018, RTO Insider, *FERC Orders Expanded Cybersecurity Reporting*, July 18, 2018. https://www.rtoinsider.com/ferc-nerc-cybersecurity-96423/

appropriate evidence generation and retention schedules, as well as impact assessment and modification to other existing programs.

In addition, most entities subject to CIP-008 are also required to document processes and report related incidents to NERC, under EOP-004, and to the U.S. Department of Energy (DOE). Recently, DOE updated its primary reporting tool to incorporate questions that are or will be included in the NERC EOP-004 Reliability Standard Event Reporting Form. With the changes to Form OE–417 if a respondent elects to have the form submitted to NERC, the entity does not need to file an EOP–004 Event Reporting Form. Form OE–417 will now collect the same information as EOP–004. By incorporating the same information, and aligning language across these two forms, entities will only be required to submit Form OE–417. This will reduce the reporting burden for the electric power industry.[2]

Unfortunately, the Commission specifically stated that it does not support adopting the DOE Form OE-417 as the primary reporting tool for reporting Cyber Security Incidents because the reporting criteria in its directive are distinguishable and more aligned with a risk management approach than the information requested in the DOE Form OE-417.[3] In addition, the accelerated (6-month) timeframe required to develop modified CIP-008 reporting requirements did not provide the time needed for the SDT to develop a more cohesive reporting approach that would satisfy EOP-004, CIP-008, and DOE in a single report. Therefore, entities are required to develop, document, and implement multiple processes to report similar information to multiple entities. Again, for smaller entities with limited staff resources, this effort may require more than 12 months to successfully achieve.

Enhanced End-User Training

In conjunction with development of new processes and associated documentation, all entities will be required to revise and augment their current training programs, as well as find the time to adequately train all personnel with key roles and responsibilities. This task is further complicated for small entities where the same person(s) may bear the responsibility to identify, report, handle, and respond to the same or similar incidents to multiple entities under multiple timelines – all while preserving the reliability of the BES. Appropriate time is needed to fully evaluate time demands, level of risk, defined roles, and reporting responsibilities and then training, as necessary to provide a sufficient level of assurance.

Responsible Entities would be best served if they are allowed to align the newly developed incident reporting and response training on the entity's current annual training cycle (CIP-004, Requirement R2).

Alignment with existing CIP-008 requirements:

In addition to an established annual training schedule, entities are required under CIP-008 Requirement R2 Part 2.1, to test their Cyber Security Incident response plan(s) on a 15-month schedule. An increased implementation timeframe affords entities the opportunity to embed the plan updates, resulting from the new reporting requirements, into their existing test schedule to achieve maximum benefit.

Network Architecture Modifications

With the additional scrutiny that Cyber Security Incidents involving attempts to compromise will likely require due to the modifications to this standard and associated definitions, entities may consider modifying current network architecture for EACMS and/or Intermediate Systems for Interactive Remote Access which may currently be used for multi-impact BES Cyber Systems (i.e., for High, Medium, and Low impact). Splitting impacts used for each EACMS and Interactive Remote Access solutions may reduce investigation and reporting burden by decreasing the attack surface by taking low-impact BES Cyber Systems out of the equation. These changes will

[2] DEPARTMENT OF ENERGY, U.S. Energy Information Administration, Agency Information Collection Extension With Changes, Federal Register /Vol. 83, No. 7 /Wednesday, January 10, 2018 /Notices.

[3] FERC Order 848 at Paragraph 73.

require deployment of additional resources, modification of many existing security processes, potential implementation of additional security controls, and coordination across large enterprises. Again, due to budgeting cycles, availability of resources, and the need for additional training, the SDT asserts that greater than 12 months is needed to successfully achieve compliance.

A few commenters stated a six-month implementation phase would be sufficient.
The SDT asserts that an 18-month implementation timeline is appropriate (see above). While in certain instances, it may be possible for some entities to implement in a shorter timeframe, the SDT asserts that entities are able to voluntarily share this information at any time, including presently.

VRF/VSLs for Requirement R4

Some commenters noted that the Violation Severity Levels (VSLs) are administrative in nature, could cause unnecessary violations, or should not have a Severe VSL.
The SDT notes that VSLs are considered for penalty sanctions after a violation has been determined based on the language of the requirement. Pursuant to the VSL Guidelines based on the 2008 FERC "VSL Order," Violation Severity Levels must have a severe category as VSLs represent degrees of compliance, not risk to the BES. A severe VSL means that an entity did not meet the performance of the requirement, whereas lesser VSLs show that an entity met some performance of the requirement but not all of the requirement. The SDT agrees that Requirement R4 is administrative in nature so it assigned a “Lower” Violation Risk Factor to reflect the requirement's impact to reliability if violated. However, this consideration does not factor into how VSLs are drafted.

Some commenters suggested the SDT move performance requirements into different VSL categories, such as assigning failure to report what had been previously defined in the first proposed draft as Reportable Attempted Cyber Security Incidents in the Moderate category and assigning a High VSL to failure to notify one of the agencies.
Based on the comments received, the SDT made several changes to the VSLs to incorporate feedback. The SDT revised the Severe VSL to be a failure to take any action under the requirement and added a High VSL to capture when an entity notifies one applicable agency of a Reportable Cyber Security Incident but did not notify the other agency. The SDT also moved failure to report attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents) to the Moderate VSL and moved other VSLs regarding Reportable Attempted Cyber Security Incidents to Lower VSL.

Other commenters recommended changes to the VSLs, such as removing Attachment 1 or Reportable Attempted Cyber Security Incidents.
The SDT determined that these comments were more appropriately addressed through considerations to revise the standard or definitions as VSLs are reflections of the requirements and must use language from the standard. In addition to revisions made in response to comments, the SDT revised the VSLs to conform to changes made to the requirements, such as deleting references to Attachment 1, and retracting the definition for Reportable Attempted Cyber Security Incidents and replacing it with requirement language for attempts to compromise, among others.

One commenter suggested revising the VSL to say an entity “did not accomplish initial notification.”
The SDT determined that the "failed to notify" language is consistent with how VSLs are often structured.

Cost Effectiveness

Many commenters expressed concern over the definition of attempts and what would be required to be reported. These commenters noted that this could dramatically increase the workload for these entities and require additional personnel to deal with the reporting requirements and timeframes.
The SDT asserts that CIP-008 is written in a way to allow entities to write a process to define an attempt that is suitable for their organization. The reporting obligations are triggered by a Responsible Entity’s determination of

reportable classification so it is meant to align with the Responsible Entity's timeline and process(es) that define reportability. The SDT asserts that the proposed 18-month implementation plan could work with entities' budget cycles should they determine a need for additional resources.

Other

Several commenters requested the Technical Rationale and Implementation Guidance document be made available at the same time the standard is balloted to provide additional information, intent, examples, and context for a clearer understanding of the requirements.
The SDT plans to post both draft Technical Rationale and draft Implementation Guidance at the time of the second ballot posting.

Several commenters expressed concern about specifying the agency name "ICS-CERT" and "or their successors," and recommended either DHS or the new agency name be used to prevent confusion.
The SDT has replaced references to "ICS-CERT" with the name of its successor entity, the "National Cybersecurity & Communications Integration Center" or "NCCIC" throughout CIP-008. The SDT retained the "or their successors" language to account for any future organization changes.

Several commenters requested clarity regarding required records retention timeframes, including types of documentation needed to demonstrate the number of "cyber ventures or trials" that were not successful reportable attempts or incidents.
As provided in Section C. Compliance, Part 1.2 Evidence Retention of CIP-008, the Responsible Entity is required to keep data or evidence to show compliance for three (3) calendar years, unless its Compliance Enforcement Agency directs a longer period of time as part of an investigation. The SDT asserts that the type of documents to retain are contingent upon each entity's incident plan and associated processes.

Several commenters requested clarity regarding use of "United States" prefacing Responsible Entity in Requirement R4.
The SDT's intent was to exempt Canadian entities from reporting to the U.S. Department of Homeland Security, and Requirement R4 has been modified to address this concern.

One commenter urged that references to "Version 5 CIP Cyber Security Standards" are updated similar to CIP-002-6.
The SDT elected to make minor revisions to the background section. Project 2016-02 will make these conforming changes to the entire suite of CIP standards at a later date.

One commenter suggested including a CIP Exceptional Circumstance (CEC) in CIP-008 with regard to the reporting timeframes.
A general review of CEC is ongoing as part of the scope of Project 2016-02.

Several commenters suggested changing the 60-day requirement for changes to roles/responsibilities, groups/individuals, or technology in Requirement Part 3.2, to 90-days as specified in Part 3.1.
The SDT asserts that modifications of these timeframes are outside of the SDT's scope of work. No changes were made to Requirement R3, and FERC Order No. 848 was silent regarding these Requirement Parts.

Several commenters suggested merging the requirements in Part 1.1 (One or more processes to identify, classify, and respond to Cyber Security Incidents) and Part 1.4 (Incident handling procedures for Cyber Security Incidents) into a new cumulative version of Part 1.1.
The SDT asserts that the only changes proposed to these Parts was to the Applicable Systems column and has elected to make no additional changes to the existing approved language.

Several commenters suggested eliminating use of the term "Responsible Entities" from Table 4, in order to align with language used in the other Tables.
Based on this comment the SDT has eliminated the use in Requirement R4, Part 4.3. The SDT asserts that the term "Responsible Entity" as used in part 4.2 is to clarify that the determination is made by the Responsible Entity in the same manner done in previously approved Table 3, Requirement R3, Part 3.2.

One commenter suggested structuring Requirement R4 similarly to other standards and removing the notifiable entities to a subpart within the Table.
The SDT asserts that Requirement R4, in its totality, covers reporting and listing the agencies in the parent Requirement helps provide clarity with regard to the requirements without the added clutter of repeating the agencies in multiple locations. Any concerns about missing the agency names should be satisfied by language incorporated into the Measures**.**

One commenter suggested adding "Reportable Attempted Cyber Security Incidents" to Requirement R3, Parts 3.1 and 3.2, requiring update of the entity's plan if it is used in response to an attempted incident.
Based on industry concern and lack of measurable statistics on the number of attempts that would be reportable as a result of the proposed modifications, as well as the exclusion of Responsible Entity determined attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents in the first proposed draft) satisfying the plan testing requirements, the SDT declines to expand the requirements in Parts 3.1 and 3.2.

A commenter supports the methods of notification, but asks the standard drafting team to include a note in the form to request receiving entities confirm receipt or provide another method of ensuring entities receive such a confirmation.
The SDT asserts that directing E-ISAC or NCCIC to provide such confirmation is not within our purview. The obligation for capturing and documenting required evidence of reporting is on the Responsible Entity. The proposed requirements do not preclude the Responsible Entity from incorporating steps into their process to request confirmation at the time of notification.

One commenter asked whether an actual "Reportable Attempted Cyber Security Incident" would be considered a test of the entity's plan under Requirement Part 2.1.
Thank you for your comment, the SDT intentionally excluded attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents in the first proposed draft) from Requirement R2, Part 2.1. Please see Technical Rationale for justification.

Several commenters requested removal of cross-references in Parts 1.2 and 4.2.
The SDT asserts the cross-referencing provides clarity and beneficial reinforcement.

One commenter suggested periodic reporting (monthly or quarterly) should be simplified, such as the IP address and service or port that was blocked, which would still provide the reporting and data necessary to meet the intent of FERC Order No. 848.
The SDT asserts that periodic reporting would not provide the timely information required by the Commission and that automated reporting would not clearly provide the required attributes.

One commenter felt that the concept of "Reportable Attempted Cyber Security Incident" is nebulous and the modifications could result in reporting with little value.
The Reportable Attempted Cyber Security Incident definition has been removed by the Standards Drafting team. Instead, the team leveraged the existing Cyber Security Incident definition, and modified the proposed CIP-008 R4, Part 4.2 language to qualify that attempts to compromise a system identified in the "Applicable Systems", including High Impact BES Cyber Systems and their associated EACMS and Medium Impact BES Cyber Systems and their

associated EACMS, are reportable after the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2.

One commenter noted that CIP-008-6 Requirement R1, Part 1.2 requires the Incident Response Plan to include processes to determine whether an incident is reportable, but does not require a documented process for notification, even though the measures for Part 1.2 reference "documented processes for notification."
The SDT addressed this comment by making modifications to the proposed standard language in Requirement R1, Part 1.2

One commenter stated that the Draft 1: CIP-008-6 Requirement R4, Part 4.3 contained a parameter and not a requirement.
The SDT agrees and modified the wording in Part 4.3 (which is now Part 4.2)

One commenter stated that the term "compromise" and "disrupt" should be included in the entity definitions that same way "programmable" is.
The SDT asserts this is outside the scope of Project 2018-02.

Several commenters raised concerns about inconsistency with the use of Reportable Attempted Cyber Security Incident and the words determined within the Measures associated with Requirement R4.
The SDT removed the proposed Reportable Attempted Cyber Security Incident definition. Instead, the team leveraged the existing Cyber Security Incident definition, and modified the proposed CIP-008 R4, Part 4.2 language to qualify that attempts to compromise a system identified in the "Applicable Systems", including High Impact BES Cyber Systems and their associated EACMS and Medium Impact BES Cyber Systems and their associated EACMS, are reportable after the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2. As a result of these modifications, the M4 verbiage was modified to match.

Several commenters raised concerns that the proposed standard has the potential to create a significant auditing burden regarding "attempts to compromise," which have no impact on reliability.
The SDT asserts that the new requirement for reporting attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incident in the first proposed draft) carries a similar evidence requirement for currently existing Reportable Cyber Security Incident.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard for formal 15-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018
20-day formal comment period with ballot	October 2018

Anticipated Actions	Date
15-day formal comment period with additional ballot	November 2018
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms:

Cyber Security Incident:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1)Electronic Security Perimeter, (2) Physical Security Perimeter, (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:

A Cyber Security Incident that has compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- Electronic Security Perimeter(s); or
- Electronic Access Control or Monitoring Systems.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to: 1.2.1 Establish criteria to evaluate and define attempts to compromise; 1.2.2 Determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident or • Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 Provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be only an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Test each Cyber Security Incident response plan 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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the 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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and Cyber Security Incident that is determined to be only an attempt to compromise a system identified in the "Applicable Systems" column.

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].*

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*.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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)[1], or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was only an attempt to compromise 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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 only an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates within 7 calendar days of determination of new or changed attribute information required in Part 4.1	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems"

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to establish criteria to evaluate and define attempts to compromise. (1.2)	column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months between tests of the plan. (2.1)	months between tests of the plan. (2.1)	months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were only an attempt to compromise a system identified in the "Applicable Systems" column for 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role	incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the	response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			ISAC or NCCIC, or their successors, within the timelines pursuant to Requirement R4, Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.3)		Requirement R4, Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Requirement R4, Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~ second draft of proposed standard for formal 15~~20~~-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018
20-day formal comment period with ballot	October 2018

Anticipated Actions	Date
~~20-day formal comment period with ballot~~	~~October 2018~~
15-day formal comment period with additional ballot	November 2018
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms:

Cyber Security Incident:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1) Electronic Security Perimeter, ~~or~~ (2) Physical Security Perimeter ~~or~~, (3) Electronic Access Control or ~~f~~ Monitoring Systems for High or Medium Impact BES Cyber Systems; ~~,~~ or ~~;~~
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber S~~s~~ystem.

Reportable Cyber Security Incident:

A Cyber Security Incident that has compromised or disrupted:

- A BES Cyber System that performs o~~O~~ne or more reliability tasks of a functional entity; ~~or~~
- Electronic Security Perimeter(s); or
- Electronic Access Control or Monitoring Systems. ~~(EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.~~

~~**Proposed New Term:**~~

~~Reportable Attempted Cyber Security Incident:~~

~~A Cyber Security Incident that was an attempt to compromise or disrupt:~~

- ~~One or more reliability tasks of a functional entity; or~~
- ~~Electronic Security Perimeter; or~~
- ~~Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting~~

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its~~-~~ documented processes~~,~~, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it~~-~~ is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to: 1.2.1 Establish criteria to evaluate and define attempts to compromise; 1.2.2 D~~d~~etermine if an identified Cyber Security Incident is: • A~~ a~~ Reportable Cyber Security Incident or • Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; ~~a Reportable Attempted Cyber Security Incident and requires notification per Requirement R4~~and ~~1.2.1~~1.2.3 Provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that ~~involves~~is determined to be only an attempt to compromise a system identified in the "Applicable Systems" column including~~s~~ justification for attempt determination criteria ~~Reportable Attempted Cyber Security Incidents~~ and documented processes for notification.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, ~~Reportable Attempted~~ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the 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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Retain records related to Reportable Cyber Security Incidents and ~~Reportable Attempted~~ Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and ~~Reportable Attempted~~ Cyber Security Incident~~s~~ that ~~involves~~ is determined to be only an attempt to compromise a system identified in the "Applicable Systems" column.

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].*

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*.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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)[1], or their successors, ~~Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and each United States Responsible Entity also shall notify the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), or their successors,~~ of a Reportable Cyber Security Incident~~s~~ and a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column~~Reportable Attempted Cyber Security Incidents~~, unless prohibited by law, in accordance with~~ing to~~ 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column -according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	~~Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, I~~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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~ICS-CERT~~NCCIC. ~~in the form of Attachment 1 submissions.~~
~~4.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~• EACMS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~• EACMS~~	~~Responsible Entities shall use one of the following methods for initial notification:~~ ~~• Electronic submission of Attachment 1;~~ ~~• Phone; or~~ ~~• Email.~~ ~~If Attachment 1 was not submitted for initial notification, it must be submitted within 5 calendar days of initial notification, without attribute information if undetermined at the time of submittal.~~	~~Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of electronic submissions of Attachment 1, phone records or email.~~

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2~~3~~	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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~~Timeline for initial notification~~: • One hour ~~from~~ after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after ~~a~~ determination that a ~~of a Reportable Attempted~~ Cyber Security Incident was only an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~ICS-CERT~~NCCIC. ~~in the form of phone records for preliminary notice or submissions through the E-ISAC and ICS-CERT approved methods, or Attachment 1 submissions.~~
4.3~~4~~	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	~~Responsible Entities shall submit~~ Provide ~~Attachment 1~~ updates ~~for the attributes required in Part 4.1~~ within 7~~5~~ calendar days of determination of new or changed attribute information required in Part 4.1~~. Submissions must occur each time new attribute information is available until all attributes have been reported.~~	Examples of evidence may include, but are not limited to, dated documentation of ~~Attachment 1~~ submissions to the E-ISAC and ~~ICS-CERT~~NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or ~~Reportable Attempted~~ a Cyber Security Incident~~s~~ that was only an attempt to compromise a system identified in the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to establish criteria to evaluate and define attempts to compromise. (1.2)	"Applicable Systems" column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Securit y Incident response plan(s) within 15 calendar months, not	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			exceeding 16 calendar months between tests of the plan. (2.1)	exceeding 17 calendar months between tests of the plan. (2.1)	exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or ~~Reportable Attempted~~ a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or ~~Reportable Attempted~~ Cyber Security Incidents that were only an attempt to compromise a system identified in the "Applicable Systems" column for 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role	120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in	The Responsible Entity notified E-ISAC and ~~ICS-CERT~~NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or ~~ICS-CERT~~NCCIC, or their successors, within the	The Responsible Entity failed to notify E-ISAC ~~or~~ and ~~ICS-CERT~~NCCIC, or their successors, of a Reportable Cyber Security Incident ~~or Reportable Attempted Cyber Security Incident~~. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Requirement R4, Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to	the "Applicable Systems" column. (R4) ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4)~~ ~~OR~~ ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber~~	~~timeframes~~ timelines pursuant to Requirement R4, Part 4.2~~3~~. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R4, Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Requirement R4, Part 4.1. (4.1) ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber~~	~~Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.~~		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4)~~ ~~OR~~ ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~to Requirement R4, Part 4.2.~~			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

~~Guidelines and Technical Basis~~

~~*Note: The Guidelines and Technical Basis section has not been revised as part of Project 2018-02. A separate technical rationale document has been created to cover Project 2018-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~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.~~

~~The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.~~

~~Requirement R2:~~

~~Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.~~

~~Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. 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."~~

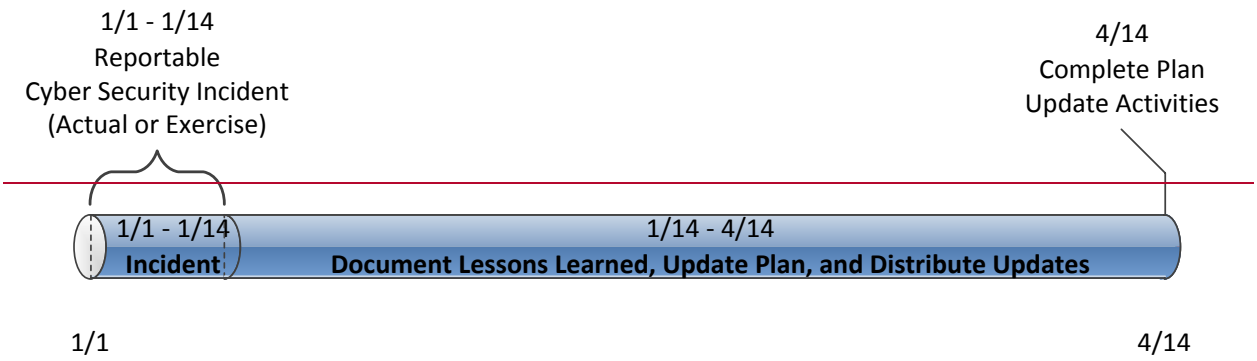
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation 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*. 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.~~

~~Requirement R3:~~

~~This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.~~

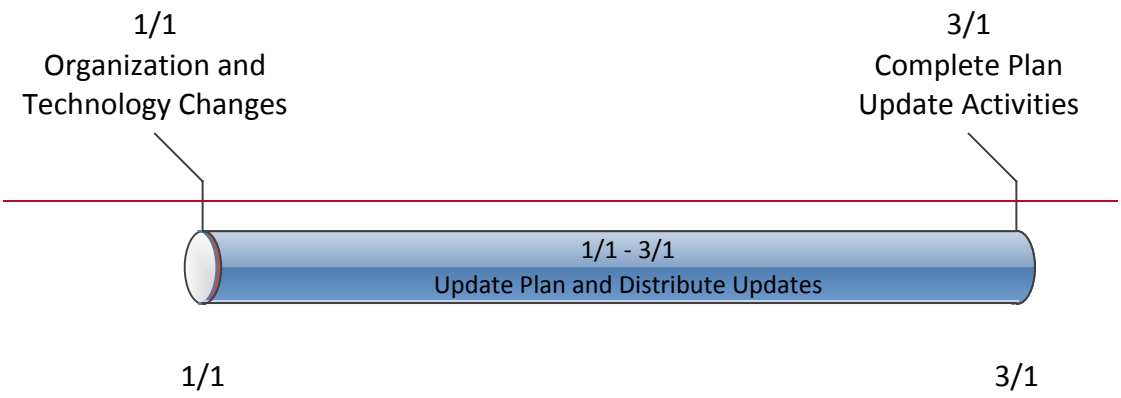
~~The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.~~



~~**Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents**~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. 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.~~

~~The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.~~



~~**Figure 2: Timeline for Plan Changes in 3.2**~~

~~Rationale:~~

~~During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.~~

~~Rationale for R1:~~

~~The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.~~

~~**Summary of Changes:** Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.~~

~~**Reference to prior version:** (Part 1.1) CIP-008, R1.1~~

~~**Change Description and Justification:** (Part 1.1)~~

~~*"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*~~

~~**Reference to prior version:** (Part 1.2) CIP-008, R1.1~~

~~**Change Description and Justification:** (Part 1.2)~~

~~*Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).*~~

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. 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.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

~~*Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*~~

~~**Rationale for R3:**~~

~~Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.~~

~~**Summary of Changes:** Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.~~

~~**Reference to prior version:** (Part 3.1) CIP-008, R1.5~~

~~**Change Description and Justification:** (Part 3.1)~~

~~*Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*~~

~~**Reference to prior version:** (Part 3.2) CIP-008, R1.4~~

~~**Change Description and Justification:** (Part 3.2)~~

~~*Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	~~10/4/18~~TBD	Modified to address directives in FERC Order No. 848	

CIP-008-6 – Attachment 1

Cyber Security Incident Reporting Form

Use this form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents in accordance with CIP-008-6, Requirement R4.

Contact Information	
Name:	
Phone Number:	

Incident Type

- ☐ Reportable Cyber Security Incident
- ☐ Reportable Attempted Cyber Security Incident

Reporting Category

- ☐ Initial Notification
- ☐ Update

Required Attribute Information

1. Attack Vector	☐ Initial	☐ Update
2. Functional Impact	☐ Initial	☐ Update
3. Level of Intrusion	☐ Initial	☐ Update

CIP-008-6 – Attachment 2

Cyber Security Incident Reporting Form Instructions

Attachment 2 provides instructions to aid in the completion of Attachment 1.

CIP-008-6—Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if Attachment 1 includes information for a Reportable Cyber Security Incident.
	Reportable Attempted Cyber Security Incident	Check this box if Attachment 1 includes information for a Reportable Attempted Cyber Security Incident. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if Attachment 1 is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if Attachment 1 is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.2.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*
	Attack Vector Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

CIP-008-6 – Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber Asset classification level.*
	Level of Intrusion Initial Checkbox	If Attachment 1 is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If Attachment 1 is being used to provide an update report, select the 'Update' checkbox.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

Requested Retirement

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New Terms in the NERC Glossary of Terms

This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the *Glossary of Terms Used in NERC Reliability Standards*.

Proposed Modified Definitions:

Cyber Security Incident:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1) Electronic Security Perimeter, (2) Physical Security Perimeter, (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; or

- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- Electronic Security Perimeter(s); or
- Electronic Access Control or Monitoring Systems.

Proposed Retirements of Approved Definitions:
Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Background

The purpose of this project is to address the directives issued by FERC in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the Reliable Operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Effective Date

Reliability Standard CIP-008-6
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.

Definition
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.

Retirement Date

Reliability Standard CIP-008-5
Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Definition
The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

Requested Retirement

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New Terms in the NERC Glossary of Terms

This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the *Glossary of Terms Used in NERC Reliability Standards.*~~Glossary.~~

~~**Proposed New Definition:**~~
~~Reportable Attempted Cyber Security Incident:~~
~~A Cyber Security Incident that was determined by the Responsible Entity to be an attempt to compromise or disrupt:~~

- ~~A BES Cyber Asset(s) that perform One or more reliability tasks of a functional entity; or~~
- ~~Electronic Security Perimeter(s); or~~

- ~~Electronic Access Control or Monitoring Systems. (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting~~

Proposed Modified Definitions:
Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1) ~~the~~ Electronic Security Perimeter, ~~or~~ (2) Physical Security Perimeter, ~~or~~ (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; ~~,~~ or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted:

- A BES Cyber System ~~Asset(s)~~ that performs ~~O~~one or more reliability tasks of a functional entity; ~~or~~
- Electronic Security Perimeter(s); or
- Electronic Access Control or Monitoring Systems. ~~(EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting~~

Proposed Retirements of Approved Definitions:
Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Background

The purpose of this project is to address the directives issued by FERC in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the R~~r~~eliable O~~o~~peration of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Effective Date

Reliability Standard CIP-008-6

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~~12~~ 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~~12~~ calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Definition

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~~12~~ 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~~12~~ 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.

Retirement Date

Reliability Standard CIP-008-5

Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Definition

The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Please note that this comment period is 15 days, with the ballot conducted the final 10 days.

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** by **8 p.m. Eastern, Thursday, November 29, 2018.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information

The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Questions

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

   ☐ Yes

   ☐ No

   Comments:

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

   ☐ Yes

   ☐ No

   Comments:

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

   ☐ Yes

   ☐ No

   Comments:

4. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? Please provide comments and an alternate approach to addressing the directive, if possible.

   ☐ Yes

   ☐ No

   Comments:

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

   ☐ Yes

   ☐ No

   Comments:

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

   ☐ Yes

   ☐ No

   Comments:

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

   ☐ Yes

   ☐ No

   Comments:

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

   ☐ Yes

   ☐ No

   Comments:

9. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

10. Provide any additional comments for the SDT to consider, if desired.

    Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-008-6. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-008-6, Requirement R1
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R1
The justification is provided on the following pages.

VRF Justification for CIP-008-6, Requirement R2
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R2
The VSL did not substantively change from the previously FERC-approved CIP-008-5 Reliability Standard. Only minor revisions were made.

VRF Justification for CIP-008-6, Requirement R3
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R3
The VSL did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VRF Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSL Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSLs for CIP-008-6, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to establish	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 1.2. (1.2)

		criteria to evaluate and define attempts to compromise. (1.2)	

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from FERC-approved CIP-008-5 and add two VSLs to the High and Severe categories to reflect new subparts 1.2.1 and 1.2.3. The two new VSLs are similar to currently-approved VSLs. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The proposed VRF is consistent among other FERC approved VRF's within the standard.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The team relied on NERC's definition of lower risk requirement.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Requirement R4, Part 4.2. (4.2)	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Requirement R4, Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Requirement R4, Part 4.1. (4.1)		successors, of a Reportable Cyber Security Incident. (R4)	

VSLs for CIP-008-6, Requirement R4			
Lower	Moderate	High	Severe

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-008-6~~[Project Number and Name or Standard Number]~~. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-008-6, Requirement R1
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R1
The justification is provided on the following pages.

VRF Justification for CIP-008-6, Requirement R2
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R2
The VSL did not substantively change from the previously FERC-approved CIP-008-5 Reliability Standard. Only minor revisions were made.

VRF Justification for CIP-008-6, Requirement R3
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R3
The VSL did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VRF Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSL Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSLs for CIP-008-6, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to establish	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 1.2. (1.2)

VSLs for CIP-008-6, Requirement R1			
Lower	Moderate	High	Severe
		criteria to evaluate and define attempts to compromise. (1.2)	

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from FERC-approved CIP-008-5 and add two VSLs to the High and Severe categories to reflect new subparts 1.2.1 and 1.2.3. The two new VSLs are similar to currently-approved VSLs. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. ~~The VRF is being established for this requirement.~~ A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion	The proposed VRF is consistent among other FERC approved VRF's within the standard.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
Guideline 3- Consistency among Reliability Standards	
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The team relied on NERC's definition of lower risk requirement.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column. (R4)	The Responsible Entity notified E-ISAC and ~~ICS-CERT~~NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or ~~ICS-CERT~~NCCIC, or their successors, within the ~~timeframes~~ timelines pursuant	The Responsible Entity failed to notify E-ISAC ~~or~~ and ~~ICS-CERT~~NCCIC, or their successors, of a Reportable Cyber Security Incident ~~or Reportable Attempted Cyber Security Incident~~. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
pursuant to Requirement R4, Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was only an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes	~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4)~~ ~~OR~~ ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.~~	to Requirement R4, Part 4.2~~3~~. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
after determination pursuant to Requirement R4, Part 4.1. (4.1) ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4)~~ ~~OR~~ ~~The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2.~~			

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs uses the same terminology as used in the associated requirement and isare, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Reporting

Technical Rationale and Justification for Reliability Standard CIP-008-6

November 2018

RELIABILITY | ACCOUNTABILITY



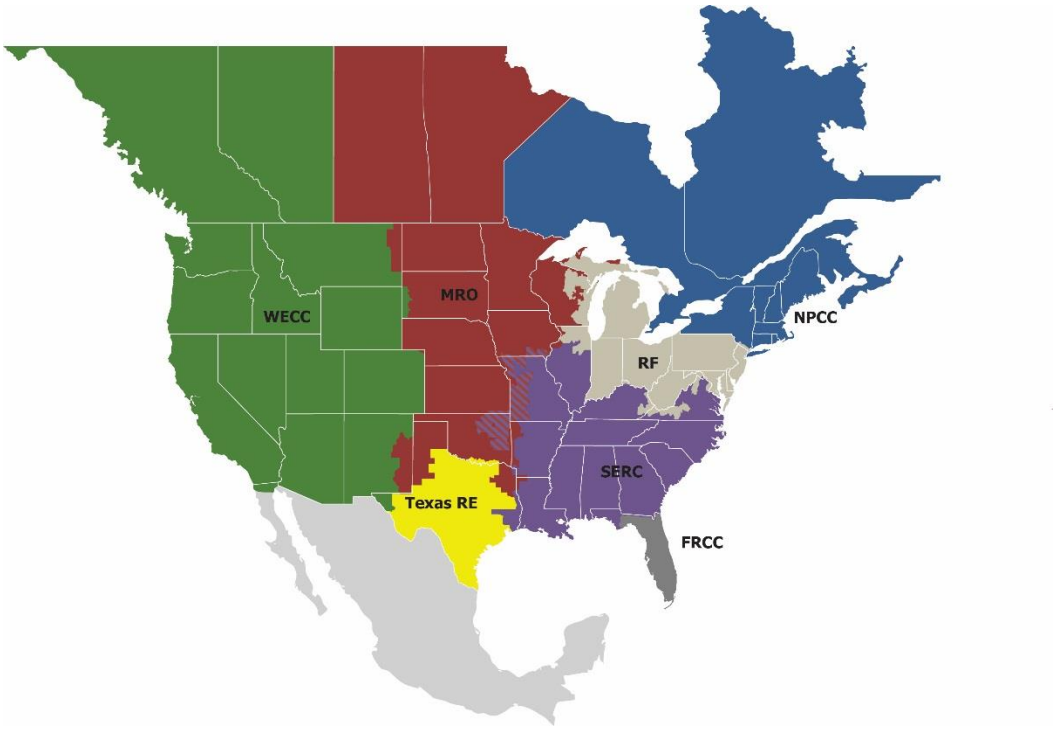

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards 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 and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)

New and Modified Terms Used in NERC Reliability Standards

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise the, (1) the Electronic Security Perimeter, (2) Physical Security Perimeter, (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems or;*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to included Electronic Access Control or Monitoring Systems (EACMS) in response to the Order.

The addition of High and Medium Impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also assures clarity and the intent to exclude Low Impact from the definition.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *Electronic Security Perimeter(s); or*
- *Electronic Access Control or Monitoring System.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for A BES Cyber System "that performs one or more reliability tasks of a functional entity" to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs).

EACMS

The drafting team spent significant time discussing this topic through industry outreach, among the team, and with FERC staff. The team believes by not specifically referencing the 5 functions in the Order, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises that entities please discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was

to minimize the changes within CIP-008 and address the required changes. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process for defining attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined criteria for determining which incidents entities must report.

The use of the language regarding Cyber Security Incident(s) being "only an attempt to compromise one or more systems identified in the "Applicable Systems" column for the Part is meant to clarify the assets for which entities are required to report attempts. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted the Requirement R1 Part 1.2 reporting requirements and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current role.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and newly-defined Reportable Attempted Cyber Security Incidents (refer to Proposed New Term, above). Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To address that, it added "to the extent known" to account for this scenario. There is an expectation that update reporting will be done as new information is determined by the entity to fill-in unknown attributes.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any approved method supported by E-ISAC and NCCIC. The SDT provided some latitude in reporting methods and format to allow responsible entities' personnel to focus on incident response itself and not the methods and format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for Reportable Attempted Cyber Security Incidents. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "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."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful penetrations of ESP(s), EACMS, or BES Cyber Asset(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was only an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at penetrating ESP(s), EACMS, or BES Cyber Asset(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day (11:59 pm local time)" was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The intent was for the timing of reporting to begin after the Responsible Entity has determined that the incident meets the reporting threshold.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.*

Back in 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[1] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one

[1] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for responsible entities to report new information over time as investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (ICS-CERT), or their successors, (and industry) upon determination of each required attribute.

The entity's process for reporting should contain a step to report until such time the entity has determined the investigation process has concluded. This allows a "closure" of this incident. At this time there is a possibility that because of circumstances, i.e. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes. In this circumstance the intent is that the entity report what is known and document the reason not all attributes could be reported.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

CIP-008 Version History from Guidelines and Technical Basis

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

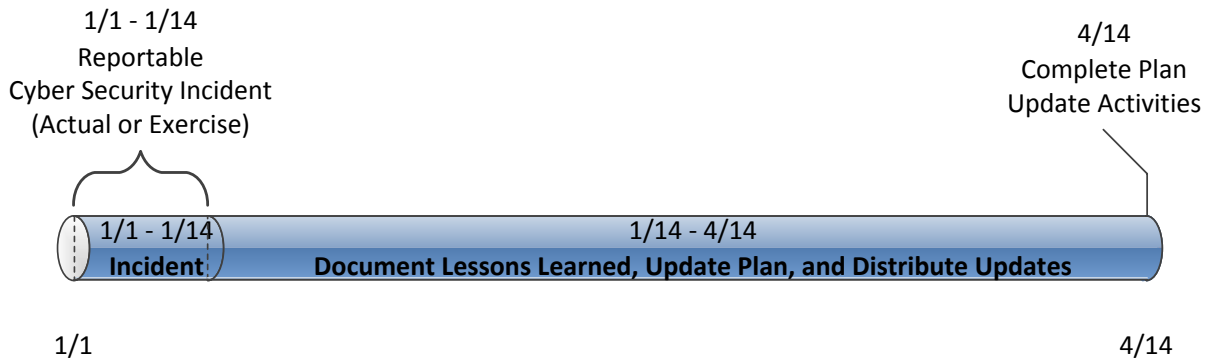
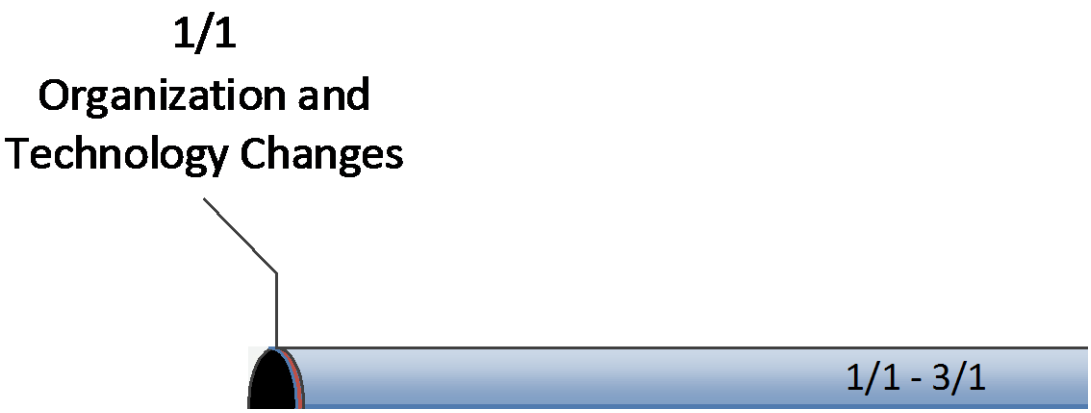


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:
The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:
The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.
This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.
Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:
Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.
Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance Pending Submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Incident Reporting and Response Planning

Implementation Guidance for CIP-008-6

RELIABILITY | ACCOUNTABILITY




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

Table of Contents

List of Figures

Introduction

The Standards Project 2018-02 – Modifications to CIP-008 Standard Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-008-6. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1]

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP- 008-6.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 848 on July 19, 2018, calling for modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.[2] The Commission directed the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the Reliability Standards 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).[3]

The Commission's directive consisted of four elements intended to augment the current Cyber Security Incident reporting requirement: (1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) now known as NCCIC[4]. Further, NERC must file an annual, public, and anonymized summary of the reports with the Commission.

The minimum attributes to be reported should 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.

The Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require responsible entities to meet the directives set forth in the Commission's Order No. 848.

---

[1] NERC's Compliance Guidance Policy

[2] 16 U.S.C. 824o(d)(5). The NERC Glossary of Terms Used in NERC Reliability Standards (June 12, 2018) (NERC Glossary) defines a Cyber Security Incident as "A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."

[3] The NERC Glossary defines "ESP" as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." The NERC Glossary defines "EACMS" as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

[4] The DHS ICS-CERT underwent a reorganization and rebranding effort and is now known as the National Cybersecurity and Communications Integration Center (NCCIC).

Definitions

CIP-008-6 has two related definitions, as well as language for "attempts to compromise" that is specific to CIP-008-6 within Requirement R1 Part 1.2.2. Cyber Security Incidents are not reportable until the Responsible Entity determines one rises to the level of a Reportable Cyber Security Incident or meets the Responsible Entity's established criteria pursuant to Requirement R1 Part 1.2.1 and 1.2.2. When these thresholds are reached reporting to both E-ISAC and NCCIC (Formerly DHS's ICS-CERT) is required. These definitions and requirement language are cited below for reference when reading the implementation guidance that follows.

Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the (1) Electronic Security Perimeter, (2) Physical Security Perimeter, (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that has compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- Electronic Security Perimeter(s); or
- Electronic Access Control or Monitoring Systems.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications		
Part	**Applicable Systems**	**Requirements**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to: 1.2.1 Establish criteria to evaluate and define attempts to compromise; 1.2.2 Determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident, or • Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 Provide notification per Requirement R4.

The determination of reportability for compromises or disruptions (by definition), or for attempts to compromise (pursuant to the requirement language), becomes a function of applying criteria that builds upon the parent definition of Cyber Security Incident.

The below Venn diagram illustrates the relationships between the elements of each definition, and the Requirement R1 Part 1.2.2 requirement language. In this example, one potential option could be to leverage the EACMS function descriptors noted in FERC Order 848 Paragraph 54 as criteria. This could serve as an approach to assess operational impact and/or functionality of cybersecurity controls that cause a Cyber Security Incident to rise to either level of reportability:

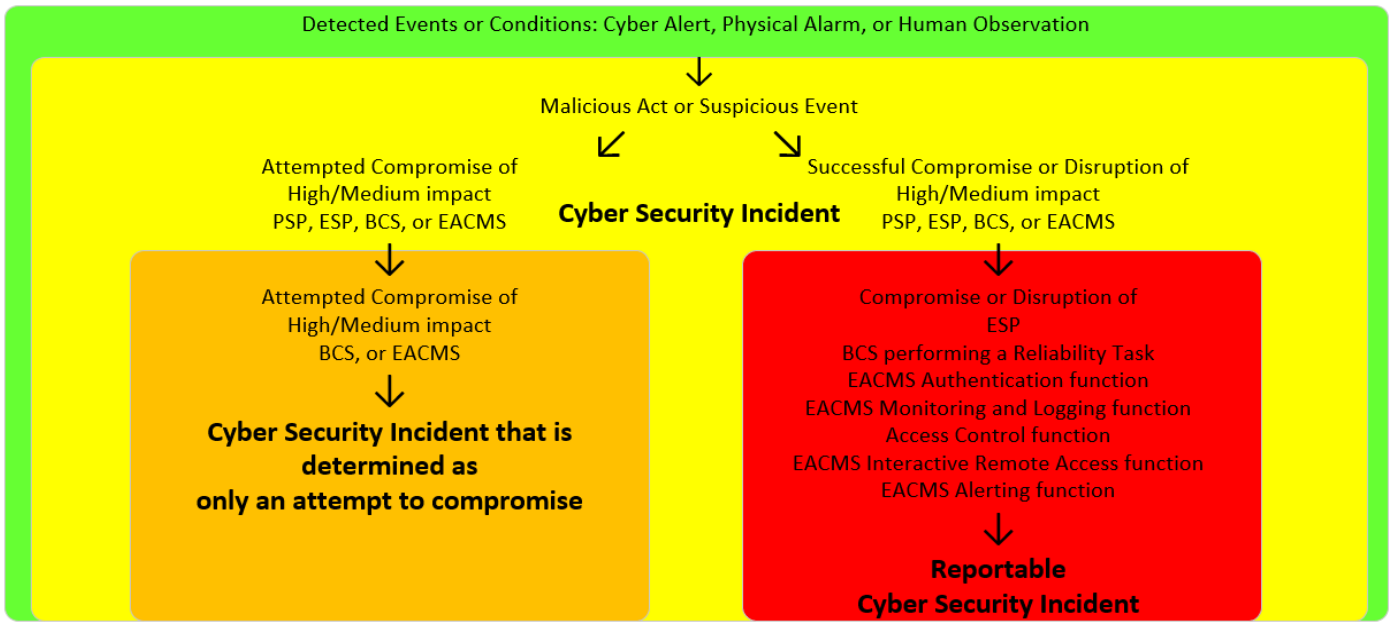


Figure 1 Relationship of Cyber Security Incidents

As shown in the above diagram, there is a progression from identification through assessment and response before a detected event or condition elevates to a reportable level.

First, the Registered Entity must determine the condition meets the criteria for a Cyber Security Incident.

Once the response and assessment has led to a Registered Entity's determination that events or conditions meet the definition of Cyber Security Incident, additional evaluation occurs to establish if established criteria or thresholds have been met for the Registered Entity to determine the Cyber Security Incident qualifies for one of the two reportable conditions:

1. Reportable Cyber Security Incident.
2. Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for Requirement R4 Part 4.2 (pursuant to Responsible Entity processes and established attempt criteria documented in accordance with Requirement R1 Part 1.2)

Once the response and investigation has led to a Registered Entity's determination that the Cyber Security Incident has targeted or impacted the BCS performing reliability tasks and/or cybersecurity functions of the Applicable Systems, associated Cyber Assets, and/or perimeters, the notification and reporting timeframes and obligations begin. Note: Initial (or preliminary) notification is needed within the specified timeframe after this determination, even if required attributes (functional impact, level or intrusion,

attack vector) are not yet known.

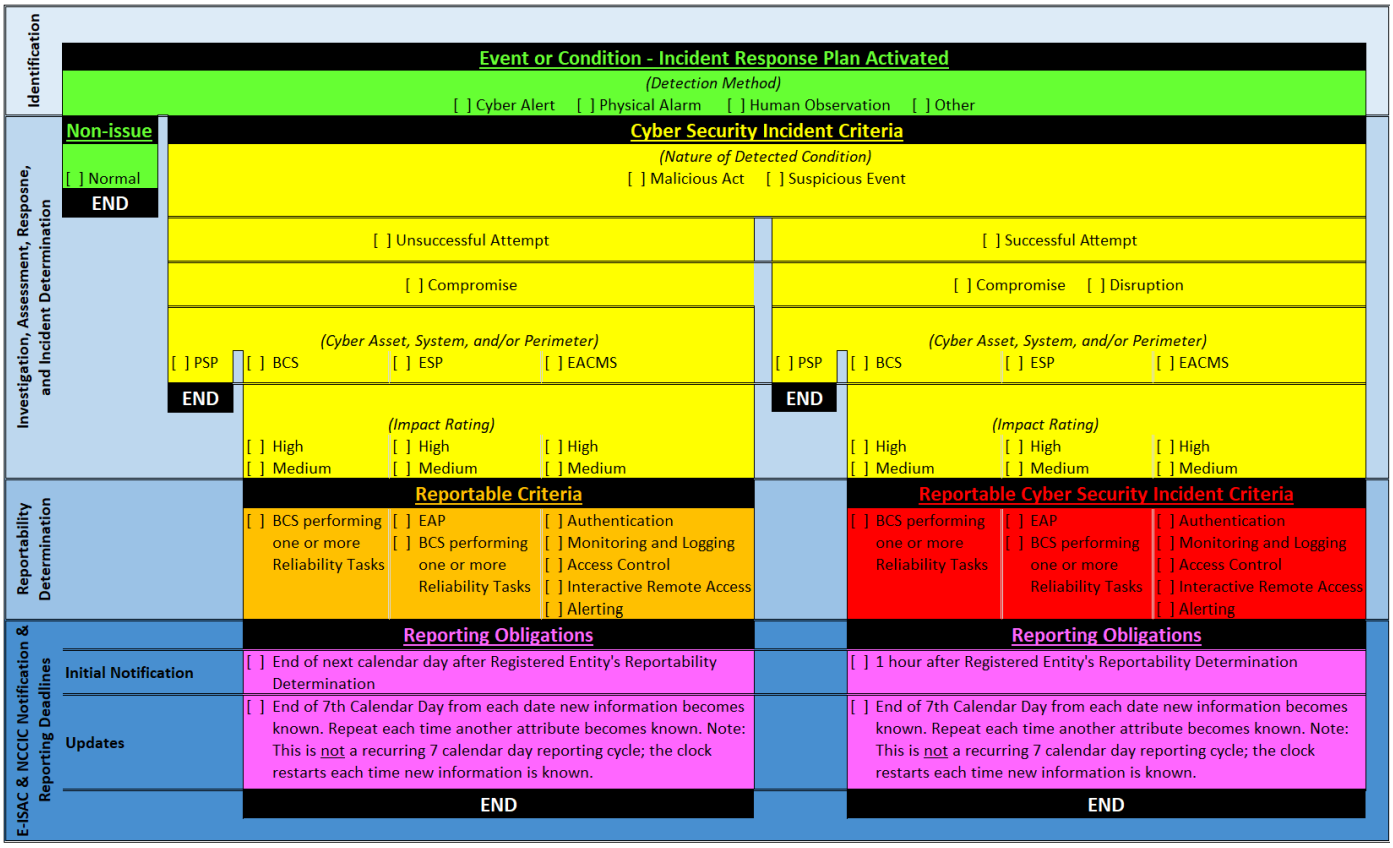
Once this initial notification is made, if all attribute were known, they should have been included in the initial notification and the reporting obligation ends.

If all attributes were not known by the time the initial notification had to be made, the update timeframes trigger from the time the next attribute(s) is learned/known.

A Registered Entity's reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC, either during the initial notification or subsequently through one or more updates made commensurate with the reporting timeframes.

Determination and Classification of Cyber Security Incidents

Registered Entities may want to consider developing tools illustrating established process criteria that must be met, by definition, as well as the impacted/targeted operational task/cybersecurity functions considered to reach each incident classification and reporting threshold. The below decision tree is one potential approach Registered Entities could employ as a tool to assess events and make the Registered Entity determinations according to process(es) and established criteria documented pursuant to Requirement R1 Parts 1.1 and 1.2.



*Where 'Calendar Day' is used, the 'end' of the day = 11:59 PM local time of that day.
** Where 'Determination' is used, this refers to the Registered Entity's Determination.

Figure 2 Potential Approach Tool

A second potential approach could be a flow diagram illustrating an entity's criteria and determination process as depicted in the example below:

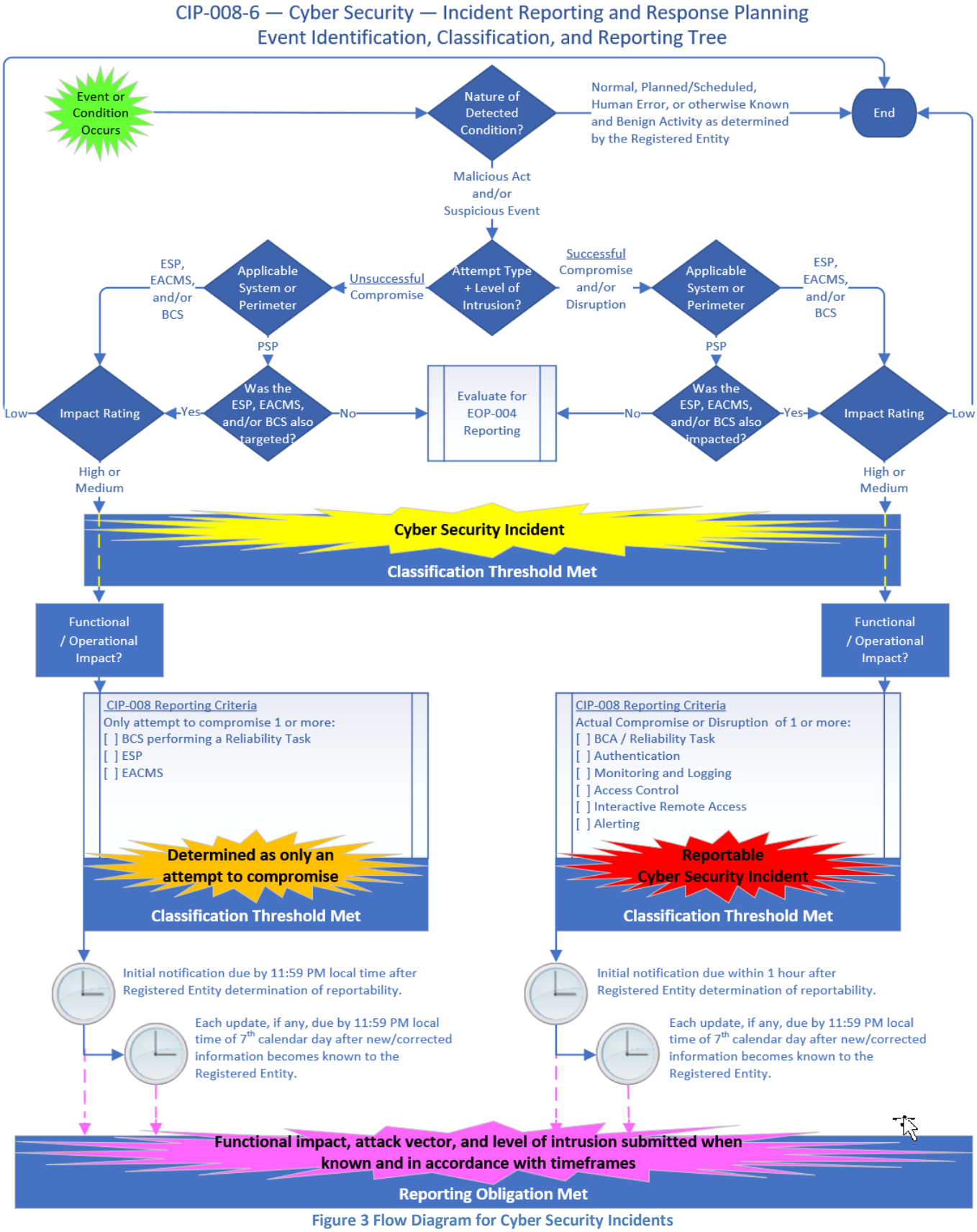


Figure 3 Flow Diagram for Cyber Security Incidents

Example of a Cyber Incident Classification Process

Entities may use a risk analysis-based method for the classification of cyber incidents and determination of Cyber Security Incidents, Reportable Cyber Security Incidents or, Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The risk analysis-based approach allows entities the flexibility to customize the appropriate response actions for their situation without being administratively burdened by a one size fits all solution. Entities also have the flexibility to incorporate their existing incident management processes which may already define how they classify and determine cyber incidents.

A risk-based approach considers the number of cyber security related event occurrences, the probability that the events will have an impact on their facilities, and severity of the impact of the event. This allows the entity to decide when cyber events should be investigated as cyber incidents, the classification of cyber incidents and the determination of when a cyber incident should be reported; either as part of a voluntary action, as part of a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

Entities should also consider that appropriate reporting of cyber incidents helps other entities in similar situations. The reporting of the details of an incident serves to alert other entities so they may increase their vigilance and take timely preventive or mitigating actions. All entities stand to benefit from such shared information in the long run.

As an example, a typical infrastructure installation is depicted in Figure below.

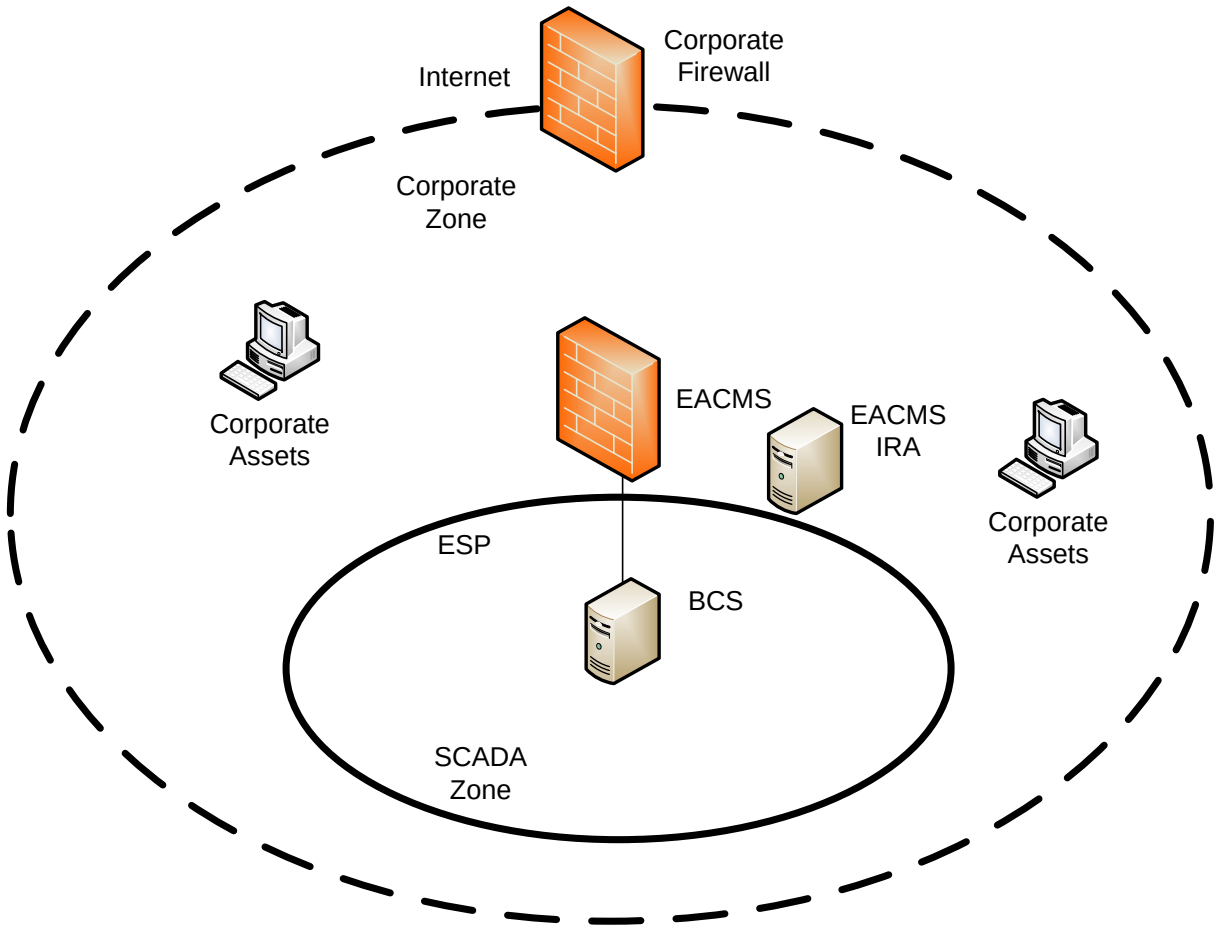


Figure 4 Typical Infrastructure

- A SCADA security zone consists of BES Cyber System (BCS), behind an Electronic Security Perimeter (ESP). The Electronic Access Point (EAP) is an interface of the SCADA firewall which is an Electronic Access Control or Monitoring System (EACMS).

- A Corporate security zone consists of regular corporate assets and other EACMS such as Intermediate Remote Access (IRA) systems. A corporate firewall protects the corporate assets against intrusions from the Internet. The SCADA security zone is nested inside the Corporate security zone.

Sample Classification Schema

A risk analysis could produce the incident categories below:

- Regular cyber events that represent a normal level of events where no further investigation is required such as random port-scans.
- Low risk incidents may be cyber events that become cyber incidents because they are beyond the normal level of events and require some type of investigation. Cyber incidents that are blocked at a firewall and found not to be malicious or suspicious could fall into this category.
- Medium risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and required mitigation activities.

  Note that while these cyber incidents were malicious or suspicious, they might not meet the definition of a Cyber Security Incident because the entity investigated and determined that the target was not a BCS, ESP, PSP or EACMS.

  For example, a corporate asset infected with well-known corporate malware and, as a result, is scanning the network to find other corporate assets. Although this activity is also being seen at the SCADA firewall (EACMS), the entity investigated and determined that this activity was not a Cyber Security Incident.
- High risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and did meet the definition of Cyber Security Incidents. For example, malicious malware on a corporate asset that repeatedly attempts to log into a SCADA IRA Intermediate System but is unsuccessful. This would be a Cyber Security Incident and should also fall into the entity's definition of a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part with the target being an EACMS (SCADA IRA Intermediate System).
- Severe risk incidents may be those Cyber Security Incidents that involves successful compromise of an ESP or EACMS and hence meet the criteria for Reportable Cyber Security Incident. These may also escalate into Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as the BCS.
- Emergency risk incidents may be those Cyber Security Incidents that compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity. These incidents may represent an immediate threat to BES reliability and may require emergency actions such as external assistance.

These incident categories can be mapped into a standard incident classification and reporting schema like the NCCIC Cyber Incident Scoring System[5]. This is a common schema used by the United States Federal Cybersecurity Centers for describing the severity of cyber incidents and is available to industry to leverage.

Utilizing the NCCIC schema as a basis for identification and classification of Cyber Security Incidents could produce the schema below for application to CIP-008-6:

	General Definition	Observed Actions	Consequences
Level 5 Emergency Black	A Cyber Security Incident that has compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity.	Effect	Incidents that result in imminent threat to public safety and BES reliability. REPORTABLE
Level 4 Severe	A Cyber Security Incident involving a compromise or disruption of an ESP or EACMS; OR Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as a BCS.	Presence or Possible Effect	Cyber Security Incidents that have the potential to result in a threat to public safety and BES reliability if malicious or suspicious activity continues or escalates. Immediate mitigation is required. REPORTABLE
Level 3 High Orange	Cyber Security Incident that attempted to compromise an EACMS.	Presence	An attempt to compromise an EACMS does not result in a threat to public safety or BES reliability, but still requires mitigation. REPORTABLE
Level 2 Medium Yellow	A cyber incident that investigation found was malicious or suspicious but was not a Cyber Security Incident because it did not target an Applicable System or perimeter.	Engagement	A cyber incident that does not represent a threat to public safety or BES reliability, even though it is malicious or suspicious and required mitigation.
Level 1 Low Green	A cyber incident that investigation found was not malicious or suspicious.	Engagement	A cyber incident that does not represent a threat to public safety.
Level 0 Baseline	Inconsequential cyber events.	Preparation	Cyber events that require no investigation and are not cyber incidents. These do not represent a threat to public safety.

Figure 5 Example of Classification Schema

Reliability tasks may be those tasks that a Responsible Entity determines are associated with the BES Reliability Operating Services (BROS) listed in the NERC Functional Model within Attachment 1 of CIP-002.

[5] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Examples of the use of the Sample Classification Schema

Some examples of the use of the classification schema are listed below. The event number corresponds to the events depicted in the subsequent figures

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
External firewall scan (N1)	External IPS log Review of F/W log	External IPS Corporate F/W rules	No	No	No	Determined by entity as regular background activity
Corporate Zone internal scan by non-malicious source (existing network monitoring Tool) (N2)	Corporate IPS Review of EACMS – IRA host F/W Log (CIP-007 R4)	Corporate IPS EACMS IRA Host F/W	No	No	No	Determined by entity as regular background activity – previously investigated and determined to be known source
Corporate Zone internal scan by unknown source (N3)	Corporate IPS Review of EACMS IRA host F/W Log	Corporate IPS IRA EACMS Host F/W	Yes	No	No	Investigation found new network monitoring tool. Added to regular background activity

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source (N4)	Corporate IPS Corporate Antivirus Review of EACMS IRA host F/W Log Review of EACMS SCADA F/W Log	Corporate IPS IRA EACMS Host F/W Corporate Anti-virus SCADA F/W EACMS	Yes	No	No	Investigation by entity determined malware in Corporate zone that was targeting other corporate assets and not the applicable systems. (via the entity's criteria to evaluate and define attempts to compromise)
Corporate Zone Internal scan by unknown source followed by EACMS IRA login attempts (N5)	Corporate IPS Review of EACMS IRA host F/W Log Review of EACMS IRA failed Logins (CIP-007 R4)	Corporate IPS EACMS host F/W EACMS login 2 factor	Yes	Yes EACMS – IRA targeted	Yes Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Investigation found malware in Corporate zone that was an attempt to compromise one or more applicable systems - IRA Intermediate System - EACMS (via the entity's criteria to evaluate and define attempts to compromise) **REPORTABLE**

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by successful EACMS IRA login and attempted BCS logins (N6)	SCADA IPS log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS failed Logins (CIP-007 R4)	SCADA IPS (CIP-005 R1.5) BCS user/ password login	Yes	Yes	Yes EACMS – IRA host compromised or disrupted Reportable Cyber Security Incident BCS host failed logins Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as BCS	Investigation found malware that compromised or disrupted EACMS IRA. **REPORTABLE** Attempt to compromise a BCS (via the entity's criteria to evaluate and define attempts to compromise) **REPORTABLE**

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
BCS – SCADA system failure following Corporate Zone Internal scan by unknown source, successful EACMS IRA login and successful BCS login (N7)	SCADA system log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS Logins (CIP-007 R4)	None	Yes	Yes	Yes Comprise or disruption of a BCS performing one or more reliability tasks of a functional entity Reportable Cyber Security Incident	Investigation found malware that compromised a BCS performing one or reliability tasks of a functional entity **REPORTABLE**

Figure 6 Examples of the Use of the Classification Schema

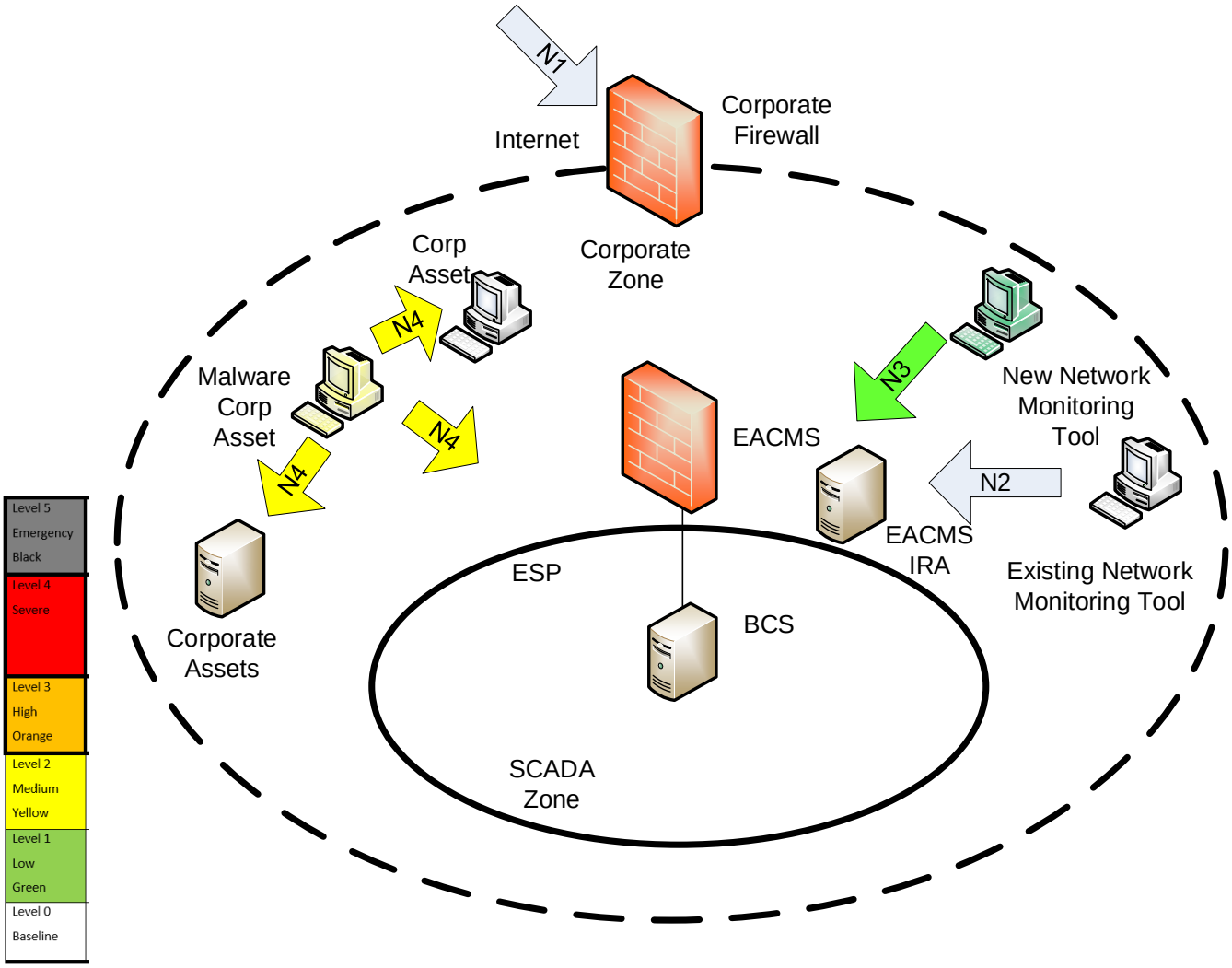


Figure 7 Examples of Non-Reportable Cyber Incidents

The figure above depicts examples of non-reportable cyber incidents using the sample classification schema and examples in Figure 6.

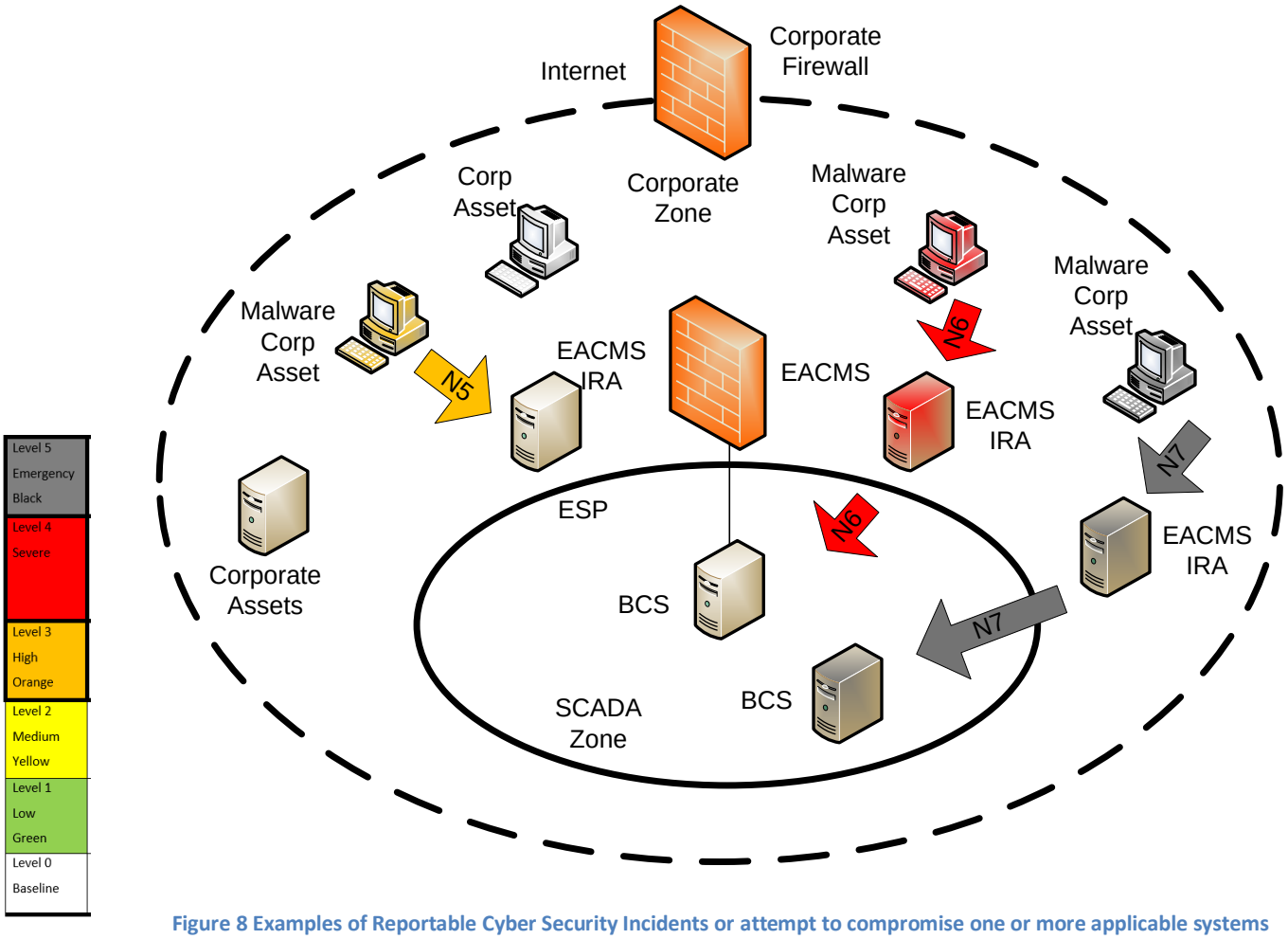


Figure 8 Examples of Reportable Cyber Security Incidents or attempt to compromise one or more applicable systems

The figure above depicts examples of Reportable Cyber Security Incidents or attempts to compromise one or more systems identified in the "Applicable Systems" column for the Part using the sample classification schema and examples in Figure 6.

Attempts to Compromise and Cyber Security Incidents

Registered Entities may want to evaluate and document what is normal within their environment to help scope and define network communications and activity that may constitute 'an attempt to compromise' in the context of CIP-008. This can help aid Subject Matter Experts (SMEs) in identifying deviations from normal, and could significantly assist a Registered Entity in timely and effective Incident determination, response, and vital information sharing. Since no two Registered Entities are alike, it stands to reason that interpretations and perspectives may vary.

Registered Entities are encouraged to explore options and tools designed to that take the guess work out of the process without being so overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs.

It is up to the Registered Entity to determine what constitutes and 'attempt to compromise', and this should be documented through the establishment of criteria that is incorporated into the Registered Entity's process. Once established, Registered Entities may want to consider incorporating a checklist to apply the defined set of criteria for SMEs to leverage as a part of the process to determine reportability.

As an example, a Registered Entity could define an "attempt to compromise" as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset in the "Applicable Systems" column. Using this sample definition:

a. Actions that are **not** an attempt to compromise an applicable Cyber Asset/System electronically are:
   i. A Registered Entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence that is performed expected on demand or on an approved periodic schedule.
   ii. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic, but it does not have malicious intent.
   iii. Attempts to access a Cyber Asset by an authorized user that have been determined to fail due to human error.

b. Actions that **are** an attempt to compromise an applicable Cyber Asset/System electronically are:
   i. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the Registered Entity's management nor process(es). This could be from an entity's own equipment due to an upstream compromise or malware.
   ii. Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.
   iii. Attempts to escalate privileges on a Cyber Asset by an authorized user that has been determined to fail due to not being authorize for that privilege level.

Registered Entities may also want to evaluate system architecture for ways to limit exposure for 'attempts to compromise'. Techniques like the implementation of security zones and/or network segmentation can minimize the level of traffic that can get to applicable Cyber Assets and help minimize the attack surface.

Registered Entities with implementations that involve an Electronic Access Control or Monitoring System (EACMS) containing both an Electronic Access Point (EAP) and a public internet facing interface are strongly encouraged to change this configuration in favor of architectures that offer layers of safeguards and a defense in depth approach.

Similarly, Registered Entities with implementations that involve an EACMS containing both an EAP and a corporate facing interface to their business networks may also want to consider options to re-architect to reduce cyber events from the corporate environment such as broadcast storms from causing extra administrative workload.

Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

The table below contains examples of various degrees of events or conditions at varied levels of determination:

Event	Normal or Benign	Malicious / Confirmed Suspicious
PSP breach	• Unauthorized user compromises the PSP to steal copper and the Registered Entity determines cybersecurity controls were not targeted and remain in place.	• Unauthorized user breaks into a Substation control house (**CIP-006-6 R1.5 activates BES Cyber Security Incident response plan within 15 minutes of detection.**)
		• Unauthorized user breaks into a Substation control house and inserts unauthorized Removable Media into an EACMS or BCS and the Registered Entity determines no interaction between the USB and the EACMS or BCS occurred. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
	• An equipment operator loses control of a backhoe and crashes into a control house, breaching the PSP and the Registered Entity determines it was accidental, cybersecurity controls were not targeted and remain in place.	• Registered Entity determines the unauthorized Removable Media contains malware (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• Registered Entity determines the malware has harvested the credentials of a BCS, gained unauthorized access and disrupted a reliability task. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)
Port Scanning	• Registered Entity owned monitoring tool that runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at the expected time.	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at an unexpected time and the Registered Entity has determined this as suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
	• A Registered Entity performs a port scan of an EACMS or BCS during a scheduled Cyber Vulnerability Assessment activity.	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it is targeting specific ports relevant to the BCS. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it gained unauthorized access to the EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)

Event	Normal or Benign	Malicious / Confirmed Suspicious
Detected malware	• A corporate machine infected by a known Enterprise Windows-specific vulnerability is scanning all local hosts including a non-Windows-based EACMS or BCS and is determined by the Registered Entity to be an SMB exploit applicable to only Windows-based machines.	• An infected corporate machine is scanning all local hosts including an EACMS or BCS for well-known ports and determined to be a suspicious event by the Registered Entity. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and has attempted to gain unauthorized access to the EACMS or BCS. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and exploited/compromised specified ICS ports that perform command and control functions of a BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)
Login activity	• Authorized user exceeded the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login attempts against an EACMS or BCS and the Registered Entity confirmed the user incorrectly entered his/her password after performing annual password changes.	• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity investigates that activity as a Cyber Security Incident deems suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**).
	• A system exceeds the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login against an EACMS or BCS and locks out a system account and the Registered Entity confirmed the system account's password had changed but the accessing application/service had not yet been updated to use the new password.	• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and failed login attempts. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**).
		• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and successfully gains unauthorized access to an EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**).

Figure 9 Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

Example of Sample Criteria to Evaluate and Define Attempts to Compromise

An entity may establish criteria to evaluate and define attempts to compromise based on their existing capabilities and facilities associated with the other CIP Standards.

The sample criteria listed below are examples and are not intended to be exhaustive.

CIP-005 R1.5:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Detected known malicious or suspected malicious communications for both inbound and outbound communications.

CIP-005 R2.1:

Require multi-factor authentication for all Interactive Remote Access sessions.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Repeated attempts to authenticate using multi-factor authentication

CIP-007 R4.1:

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;
4.1.2. Detected failed access attempts and failed login attempts;
4.1.3. Detected malicious code.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Successful login attempts outside of normal business hours
- Successful login attempts from unexpected personnel such as those who are on vacation or medical leave
- Detected failed access attempts from unexpected network sources
- Detected failed login attempts to default accounts
- Detected failed login attempts from authorized personnel accounts exceeding X per day

- Detected failed login attempts from authorized personnel accounts where the account owner was not the source
- Detected malicious code on applicable systems

CIP-007 R5.7:

Where technically feasible, either:

- *Limit the number of unsuccessful authentication attempts; or*
- *Generate alerts after a threshold of unsuccessful authentication attempts.*

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Account locked due to limit of unsuccessful authentication attempts exceeded more than X times per day
- Threshold of unsuccessful authentication attempts exceeds more than X every Y minutes

CIP-010 R2.1:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Detected unauthorized changes to the baseline configuration

An entity may establish additional criteria to evaluate and define attempts to compromise based on their infrastructure configuration:

Sample criteria:
Where investigation by entity determines that the specific activity, while malicious or/and suspicious:

- Attempt to compromise was not intended to target the “Applicable Systems”

Requirement R1

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].*

1.1. One or more processes to identify, classify, and respond to Cyber Security Incidents.

1.2. One or more processes:

1.2.1. Establish criteria to evaluate and define attempts to compromise;

- Determine if an identified Cyber Security Incident is A Reportable Cyber Security Incident or
- Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; and

1.2.2. Provide notification per Requirement R4.

1.3. The roles and responsibilities of Cyber Security Incident response groups or individuals.

1.4. Incident handling procedures for Cyber Security Incidents.

General Considerations for R1

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

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 no 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.

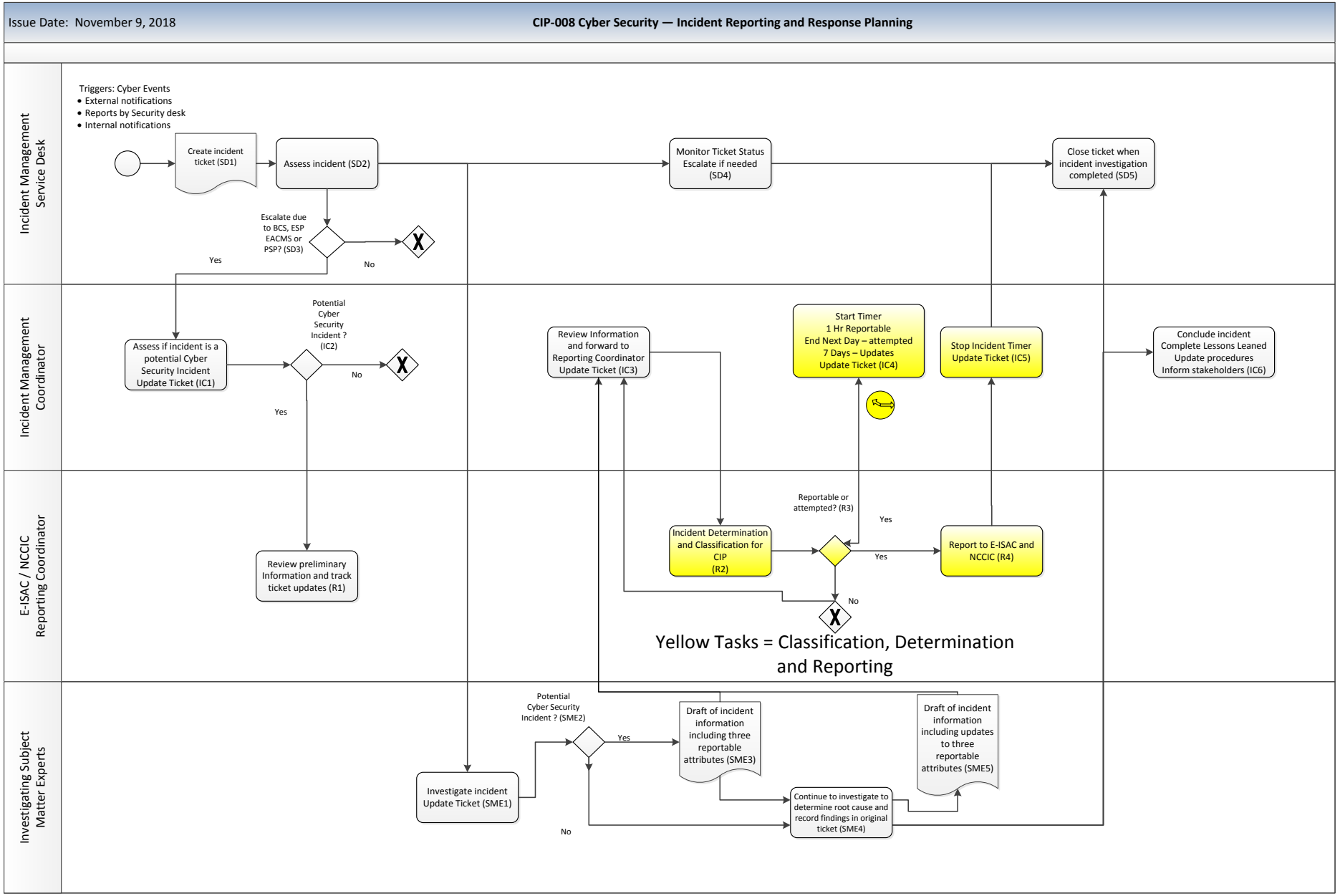


Figure 10 Sample Process to Identify, Classify and Respond to Cyber Security Incidents

Supporting Narrative Description of Sample Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

1. The Incident Management Service Desk identifies that a cyber event that requires investigation has occurred.
2. Incident Management Service Desk creates an incident ticket to log the suspected cyber incident (SD1).
3. Incident Management Service Desk performs initial assessment of the suspected cyber incident and performs any initial triage or service restoration as needed (SD2).
4. If the suspected cyber incident involves BES Cyber Systems (BCS), Electronic Access Control or Monitoring Systems (EACMS), Electronic Security Perimeter (ESP) or Physical Security Perimeters (PSP), the Incident Management Service Desk will escalate the incident to an Incident Management Coordinator whom will act as the coordinator until the incident is closed (SD3)
5. The Incident Management Coordinator performs a secondary initial assessment to determine if the incident has the potential to be a Cyber Security Incident, a Reportable Cyber Security Incident, or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

   They update the incident ticket, assigning the appropriate Investigating Subject Matter Experts (IC1).
6. If the Incident Management Coordinator determines that the incident has the potential to be reportable, the E-ISAC/ NCCIC Reporting Coordinator is alerted and copied on the information contained in the incident ticket. The E-ISAC/ NCCIC Reporting Coordinator continues to monitor the updates to the incident ticket (IC2)
7. The Incident Management Service Desk ensures the assigned Investigating SMEs are notified, and the incident ticket information is updated (SD2, SD4)
8. The assigned SMEs investigate the incident ticket updating with the Incident Management Coordinator as appropriate (SME1). The Incident Management Coordinator will monitor the progress of the investigation and assign additional SMEs or escalate as needed.
9. If initial investigation by SMEs finds that the incident may be a Cyber Security Incident and has the potential to be reportable (SME2), the SMEs will inform the Incident Management Coordinator and forward the known information including the required three attributes (SME3). Attributes which are unknown at the current time will be reported as "unknown".
10. The SMEs will continue their investigation to determine the root cause of the incident, performing triage or service restoration as needed, continue to investigate the three required attributes and update incident ticket information (SME4).
11. If the incident is found to be potentially reportable, the Incident Management Coordinator reviews the information, adds any details collected by other investigating SMEs and resolves any missing information as needed. The information is forwarded to the E-ISAC/ NCCIC Reporting Coordinator (IC3)
12. The E-ISAC/ NCCIC Reporting Coordinator reviews the information received, performs classification of the incident (R2). They determine if the incident is a Cyber Security Incident and determine if it is either a Reportable Cyber Security Incident or Cyber Security Incident that attempted to compromise

a system identified in the "Applicable Systems" column for the Part. The information to be reported is finalized (R3).

13. Upon determination that the incident is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a clock timer set to the appropriate time frame (IC4) and performs the required notification including the three required attributes. The incident ticket is updated with the incident classification and determination time for compliance evidence purposes:
    - Within 1 hour for initial notification of Reportable Cyber Security Incident,
    - By end of the next day for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part,
    - Within 7 calendar days of determination of new or changed attribute information required in Part 4.1

14. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator when notification is completed and time that the notifications occurred at. The Incident Management Coordinator will stop the appropriate timer and updates the incident ticket with the appropriate information for compliance evidence purposes (IC5)
15. If Incident Management Coordinator that has not received confirmation of notification, they may escalate, as needed, prior to expiry of the applicable timer. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4)
16. During the continued investigation of the incident (SME4), the SMEs may find that an update of any of the three required attributes is potentially required. The SMEs will inform the Incident Management Coordinator and forward a draft of the updated information (SME5)
17. The Incident Management Coordinator reviews the draft update information including adding other details, and then informs E-ISAC/ NCCIC Reporting Coordinator, forwarding the potential update information (IC3)
18. The E-ISAC/ NCCIC Reporting Coordinator reviews the potential updated information and determines if the update to any of the three required attributes is reportable (R3).
19. Upon determination that the update is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a timer set to the appropriate time frame (i.e. 7 calendar days). The incident ticket is updated with the determination time for compliance evidence purposes (IC4)
20. The E-ISAC/ NCCIC Reporting Coordinator updates both E-ISAC and NCCIC with the information associated with any of the three required attributes (R4)
21. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator that the update to E-ISAC and NCCIC is completed and times that the updates occurred at. The Incident Management Coordinator will stop the appropriate timer and update the incident ticket with the appropriate information for compliance purposes (IC5)

22. If the Incident Management Coordinator that has not received confirmation of the update being completed, prior to the expiration of the timer, they may escalate as needed. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4)
23. Upon closure of the incident, the Incident Management Coordinator will ensure that the last reportable update to the three required attributes accurately reflects the closure information. If a further update of the three required attributes is required, the Incident Management Coordinator will inform the appropriate Subject Matter Expert to initiate an update (SME5).
24. The Incident Management Coordinator informs the Incident Management Service Desk that the incident ticket may be closed (SD5).
25. The Incident Management Coordinator will initiate a "Lessons Leaned" session and update to the Cyber Incident Reporting and Response Plan and any other documentation, procedures, etc. within 90 days (IC6). They will inform all stakeholders of any updates to the Cyber Incident Reporting and Response Plan and any other applicable documentation

Roles and Responsibilities (R1.3)

In the example process, the defined Roles and Responsibilities are as follows, but can be tailored by any entity to align with their unique organization:

- Incident Management Service Desk is responsible for initial activities, incident ticketing and incident logging:
    - Initial identification, categorization and prioritization,
    - Initial diagnosis and triage/service restoration,
    - Initial assignment of incident tickets to Investigating Subject Matter Experts (SMEs)
    - Initial escalation to an Incident Management Coordinator upon assessment (if needed)
    - Monitoring incident ticket status and initiating further escalation (if needed)
    - Incident ticket resolution and closure
    - General incident status communication with the user community

- Incident Management Coordinator is responsible for the over-all coordination of activities related to an assigned incident:
    - Detailed assignment of tasks to Investigating SMEs
    - Ensure that all assigned activities are being performed in a timely manner
    - Ensuring regulatory reporting time limits are met and initiating escalation if needed
    - Communicating incident status with major affected stakeholders
    - Coordinating with the Incident Management Service Desk to update incident tickets with status and the logging of required details and assisting them to perform general incident status communications with the user community

- Coordinating with the E-ISAC/NCCIC Reporting Coordinator for cyber incidents with the potential of being Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Assisting the E-ISAC/NCCIC Reporting Coordinator with information to aid in the classification of the cyber incident.
- Escalation as needed according to the priority and severity of the issue
- Coordination of service restoration and incident closure
- Coordination of incident review following closure of incidents, identification of potential problems and documenting the "Lessons Learned"
- Initiating update of processes or procedures as needed and communicating the updates to stakeholders

- E-ISAC/ NCCIC Reporting Coordinator is responsible for the coordination of regulatory reporting activities such as those related to E-ISAC and NCCIC:
  - Review of completeness incident information for classification and reporting purposes
  - Incident classification for reporting purposes
  - Determination if this incident is a Cyber Security Incident, Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part
  - Completeness of the required three attributes to be reported
  - Notification to E-ISAC and NCCIC and submission of the three required attributes
  - Coordinating with Incident Management Coordinator to ensure timing is in accordance with regulatory requirements and that incident logging is complete for compliance evidence purposes

- Investigating Subject Matter Experts are responsible for detailed technical tasks related to the investigation of the incident and performing the needed recovery actions:
  - Perform investigation tasks related to the incident as assigned by the Incident Management Coordinator to determine the root cause of the incident
  - Perform service restoration tasks related to the incident as assigned
  - Update incident ticket and ensure all required details are logged
  - Obtaining information on the three required attributes for both initial notification and updates
  - After incident closure, participate in "Lessons Learned" sessions and update procedures as needed

Incident handling procedures for Cyber Security Incidents (R1.4)

Each of the defined roles in the example process may have specific procedures covering various aspects of their tasks being accomplished within the process. The sample process documents "what" the overall required steps are whereas the procedures document "how" each step is carried out:

- Incident Management Service Desk Procedures:
    - Procedures of when to classify cyber events as possible cyber incidents
    - Procedures to determine if BCS, PSP, ESP or EACMS are involved and decision criteria of when to escalate to an Incident Management Coordinator.
    - Procedures for initial diagnosis, triage and service restoration
    - Procedures for incident ticketing, assignment, escalation and closure

- Incident Management Coordinator Procedures:
    - Procedures for finding if cyber events or incidents could be possible Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. These potential incidents require notification to the E-ISAC/ NCCIC Coordinator
    - Procedures for the assignment and tracking of tasks to Investigating SMEs
    - Procedures associated with regulatory reporting time limits
    - Procedures for incident review, documentation of lessons learned, tracking of completion of documentation update status
- E-ISAC/ NCCIC Reporting Coordinator Procedures:
    - Procedures on how to use the Entity's own classification and reporting schema to classify cyber incidents and determine Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part
    - Procedures on the review of information to be used for reporting the three required attributes to be included for E-ISAC or NCCIC notification including the handling of any BES Cyber System Information
    - Procedures for the notification of updates to E-ISAC and NCCIC including the submission of the three required attributes
- Investigating Subject Matter Experts Procedures:
    - Procedures for the classification of cyber incidents to possible Cyber Security Incidents, possible Reportable Cyber Security Incidents or possible Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part and the required information needed to be obtained.
    - Procedures for troubleshooting tasks to determine root cause of an incident

- Procedures for service restoration tasks after an incident
- Procedures for triggering the forensic preservation of the incident
- Procedures on when updates are necessary to information on the required attributes associated with a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for the Part

Requirement R2

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]*

2.1. 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.

2.2. Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the 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.

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.

General Considerations for R2

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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, multi-discipline 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. 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.

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[6]. 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.

[6] 2009, Department of Homeland Security, Developing an Industrial Control Systems Cybersecurity Incident Response Capability, page 13.

Requirement R3

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].*

3.1. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:

3.1.1. Document any lessons learned or document the absence of any lessons learned;

3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and

3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

3.2. No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:

3.2.1. Update the Cyber Security Incident response plan(s); and

3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.

General Considerations for R3

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

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.

Requirement R4

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 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].*

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 within 7 calendar days of determination of new or changed attribute information required in Part 4.1

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"

NCCIC Reporting

NCCIC reporting guidelines for reporting events related to Industrial Control Systems can be found here:

https://ics-cert.us-cert.gov/Report-Incident

https://www.us-cert.gov/incident-notification-guidelines

NCCIC prefers the reporting of 10 attributes, although they will accept any information that is shared. A potential mapping between the NCCIC preferred attributes and the attributes required to comply with CIP-008-6 standard could be represented are as follows:

CIP-008-6 Reporting	NCCIC Reporting	Comment
Functional Impact	Identify the current level of impact on agency functions or services (Functional Impact).	
Functional Impact	Identify the type of information lost, compromised, or corrupted (Information Impact).	
Functional Impact	Identify when the activity was first detected.	
Level of Intrusion	Estimate the scope of time and resources needed to recover from the incident (Recoverability).	
Level of Intrusion	Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident	
Level of Intrusion	Identify the number of systems, records, and users impacted.	
Level of Intrusion	Identify the network location of the observed activity.	
Level of Intrusion	Provide any mitigation activities undertaken in response to the incident.	
Attack Vector	Identify the attack vector(s) that led to the incident.	
Name and Phone	Identify point of contact information for additional follow-up.	

Figure 11 NCCIC Reporting Attributes

Example of a Reporting Form

Entities may wish to create an internal standard form to be used to report Reportable Cyber Security Incidents and Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The advantages of using a standard internal form are:

- A standard internal format for the communications of cyber incident information between the various internal roles with respect to obligations of CIP-008-6, Requirement R4
- A standard written record of the notification of the minimum 3 attributes having been reported to E-ISAC and NCCIC in accordance with CIP-008-6, Requirement R4 which can be easily stored, sorted and retrieved for compliance purposes

An example of an internal standard form is shown. The instructions on how to complete this form are included after it.

CIP-008-6 Requirement R4

Cyber Security Incident Reporting Form

This form may be used to report Reportable Cyber Security Incidents and Cyber Security Incidents that were an attempt to compromise a system listed in the "Applicable Systems" column for the Part.

Contact Information

Name: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

Click or tap here to enter text.

Instructions for Example of a Reporting Form

These are instructions on how to complete the optional form

CIP-008-6
Cyber Security Incident Reporting Form Instructions

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if report includes information for a Reportable Cyber Security Incident.
	Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Check this box if report includes information for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if report is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if report is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.3.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
	Attack Vector Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber System classification level.*
	Level of Intrusion Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If report is being used to provide an update, select the 'Update' checkbox.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2018-02 Modifications to CIP-008

Cyber Security Incident Reporting

Standard Drafting Team Meeting
September 17, 2018 2:00-4:00 p.m. Eastern

RELIABILITY | ACCOUNTABILITY




NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Kick-off

RELIABILITY | ACCOUNTABILITY




Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement
- Roll Call and Determination of Quorum

Agenda Items

- Chair/Vice Chair Introductions and Remarks
- Review FERC Order 848
- Review Standards Process
- Objectives for First in-person meeting
- Review Project Timeline
- Future In-person Meetings (Sept 24-26, November 6-8, December 11-13)
- Adjourn

Administrative / Introductions

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement
- Roll Call and Determination of Quorum

Introductions

- Chair/Vice Chair Introductions and Remarks, and team introductions

Dave Rosenthal (C)	Kristine Martz (VC)	Steve Brain
Sharon Koller	Norm Dang	John Gasstrom
Tina Weyand	Tony Hall	Jennifer Korenblatt
John Breckenridge	Ian King	Katherine Anagnost

Alison Z. Oswald – NERC Sr. Standards Developer

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 848

RELIABILITY | ACCOUNTABILITY




Order Dates

- Order Issue Date: July 19, 2018
- Order Fed. Reg. Publish Date: July 31, 2018
- Order Effective Date: October 1, 2018
- Directive Filing Deadline: April 1, 2019

Modifications Directed

1. Augment reporting to include Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems

2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information

Modifications Directed Continued

3. Filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a Responsible Entity

4. Reports should continue to be sent to the E-ISAC, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

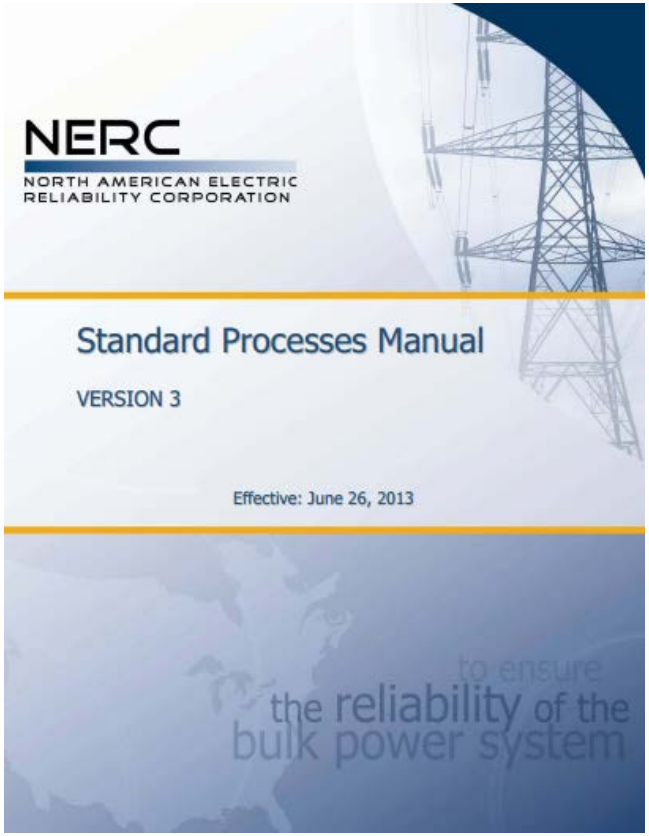
Standards Development Process

RELIABILITY | ACCOUNTABILITY




NERC's Standards Development

- Governed by the Rules of Procedure, Appendix 3A: Standard Processes Manual (SPM) - Version 3, effective June 26, 2013



Roles and Responsibilities of Drafting Teams

- Develop an excellent, technically correct standard that helps provide an adequate level of reliability and achieves consensus
  - Stay within the scope of the SAR
  - Address regulatory directives and stakeholder issues
  - Consider Independent Experts' Review Panel input
  - Ensure standard meets criteria for approval
- Develop modifications of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) and associated reasoning
- Develop Implementation Plan
- Develop supporting documents (optional)
- Outreach

Drafting Team Formation and Support

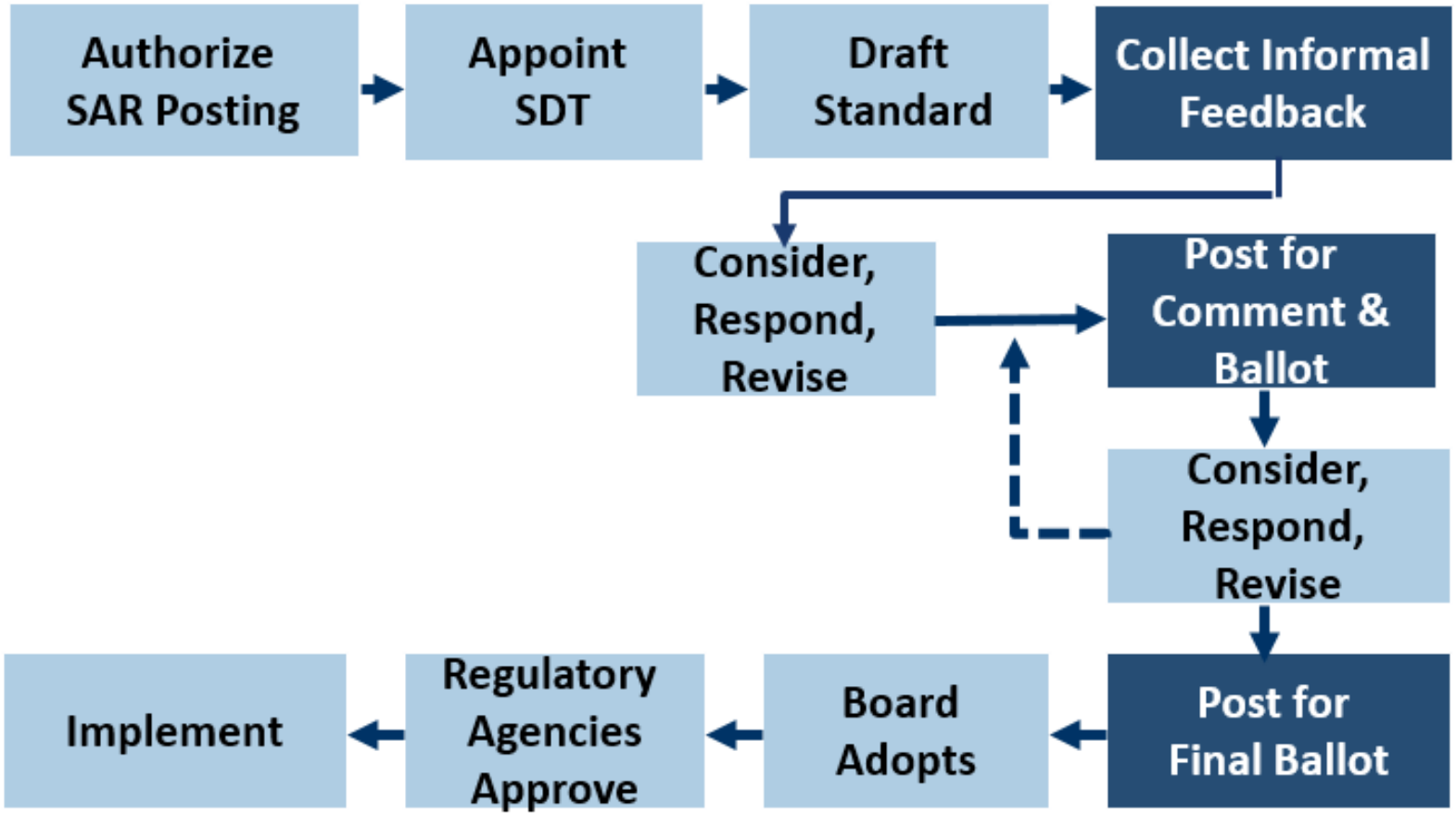
- Drafting team chair and vice chair
- NERC standards developer
- Subject Matter Experts (SMEs)
- Legal
- FERC staff observers
- Industry observers

Drafting Team Training

- All Standards Drafting Team members must complete training
  - Two modules
    - Module 1: How to Develop a High Quality Standard
    - Module 2: Your Role on a Drafting Team and Outreach

  - Send Certificate when training is complete

NERC Standards Development Process



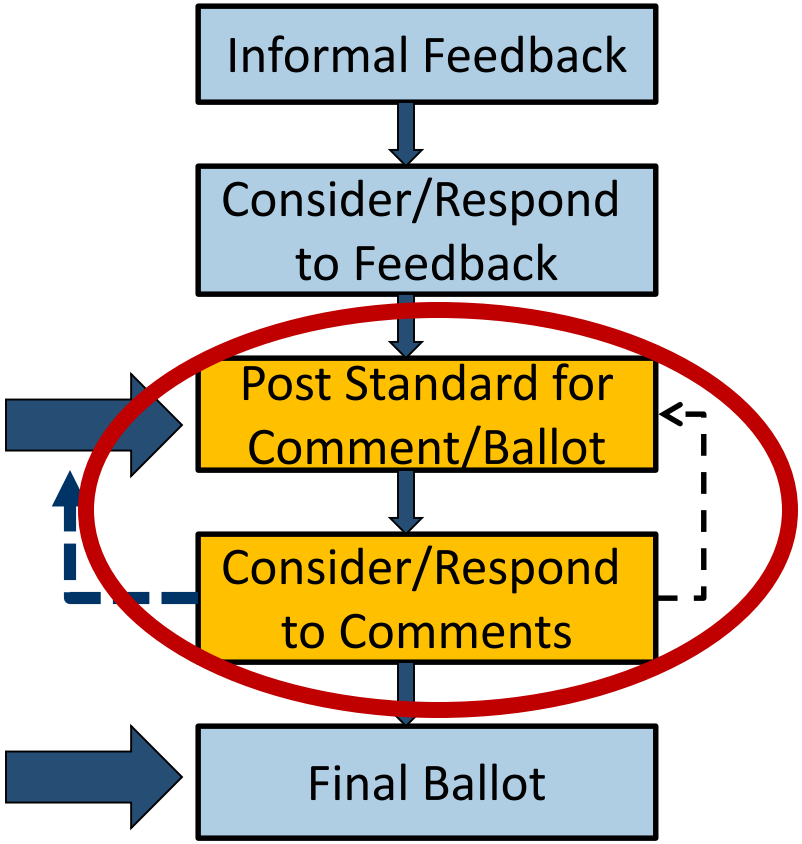
Stakeholder Consensus Process

Initial/Additional Ballot:

At this step, the standard is either "new" or significantly changed from the last version posted for comment/ ballot.

Final Ballot:

At this step, there have been no significant changes to the standard from the last ballot. The ballot record starts with all votes and comments from the previous ballot.



Initial/Additional Comment Period and Ballot

Typically 45-day period

- 45-day comment period
- 10-day ballot
- These periods may vary due to:
  - Waivers necessary to meet regulatory directives or NERC Board deadlines

Consideration of Comments

- The drafting team must communicate changes to stakeholders

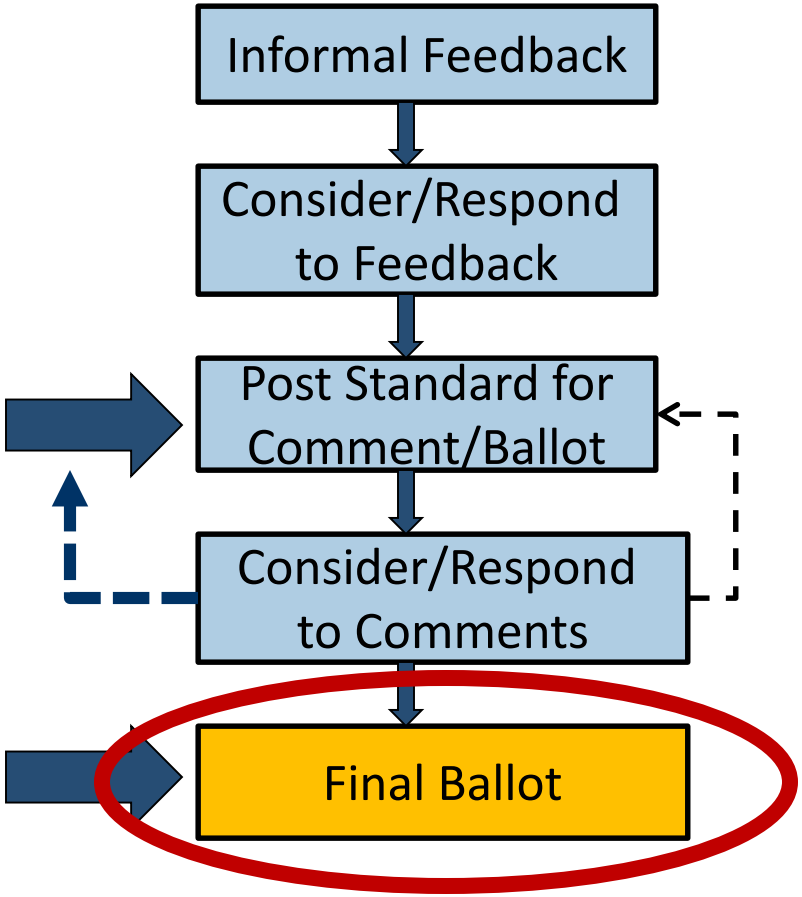
Stakeholder Consensus Process

Initial/Additional Ballot:

At this step, the standard is either "new" or significantly changed from the last version posted for comment/ ballot.

Final Ballot:

At this step, there have been no significant changes to the standard from the last ballot. The ballot record starts with all votes and comments from the previous ballot.



Objectives for Meeting #1

Be Prepared!!!

- For our first in person meeting, please bring:
  - Options for draft language
    - Not just requirement language but for incident reporting form
  - Potential mock-up of draft incident reporting form
  - Pain points where people believe there will be issues
    - This can notional, but we need to get ahead of our challenges
- There will be a public posting after the first meeting
  - Draft requirement language, incident reporting form as well as:
    - Draft implementation plan
    - Comment form that is used with the first public posting
- Leverage outreach AND your company/associations
  - Again, please come prepared

Project Timeline

Anticipated Date	Location	Event	Comments
September 17, 2018	Conference Call	SDT Webex	Introduce team, review objectives for first meeting
September 24-26, 2018	Atlanta, GA	SDT in-person meeting to modify the CIP-008-5 standard	
September 27, 2018	-	Quality Review and Admin Review	
September 28, 2018	Conference Call	SDT Meeting to review feedback from Quality Review	
October 4 – 23, 2018	-	Post CIP-008 Standard for 20-day comment and ballot	
Week of October 15, 2018	Conference Call	Webinar to educate industry on changes	
October 24-November 2, 2018	-	Consolidate comments and distribute to team	Team conference call to assign comments to members to address
November 6-8, 2018	TBD	Second SDT in-person meeting to respond to comments and modify as necessary	
November 9, 2018		Quality Review and Admin Review	
November 13, 2018	Conference Call	SDT Meeting to review feedback from Quality Review	
November 14 – 28, 2018	-	Post for an additional comment and ballot	Waiver of the time frame to shorten from 45 days to 15 days.
November29 - December 7, 2018	-	Consolidate comments and distribute to team	Team conference call if necessary to assign comments to members to address
December 11-13, 2018	TBD	SDT Meeting to respond to comments and move to a final ballot	
January 14 – 18, 2019	-	Post for Final Ballot	Shortened to 5 days.
February 6-7, 2019	-	NERC Board of Trustees Adoption	
February 2019	-	NERC Files Petition with the Applicable Governmental Authorities	

Future In-Person Meetings

- September 24-26, 2018
  - Atlanta, GA at NERC office
  - begin at 1pm, end at 3pm
- November 6-8, 2018
  - Location TBD
- December 11-13, 2018
  - Location TBD

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

15-day Formal Comment Period Open through November 29, 2018

Now Available

A 15-day formal comment period for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** is open through **8 p.m. Eastern, Thursday, November 29, 2018.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues using the SBS, contact Wendy Muller**.** An unofficial Word version of the comment form is posted on the project page**.**

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

A 10-day additional ballot for the standard, and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 20-29, 2018**.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/159)
Ballot Name: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 AB 2 ST
Voting Start Date: 11/20/2018 12:01:00 AM
Voting End Date: 11/29/2018 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 306
Total Ballot Pool: 324
Quorum: 94.44
Quorum Established Date: 11/29/2018 12:16:04 PM
Weighted Segment Value: 75.54

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	90	1	65	0.793	17	0.207	0	4	4
Segment: 2	7	0.7	2	0.2	5	0.5	0	0	0
Segment: 3	72	1	51	0.836	10	0.164	1	4	6
Segment: 4	18	1	14	0.824	3	0.176	0	0	1
Segment: 5	74	1	53	0.815	12	0.185	1	6	2

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	53	1	36	0.818	8	0.182	0	4	5
Segment: 7	1	0.1	0	0	1	0.1	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	8	0.7	6	0.6	1	0.1	0	1	0
Totals:	324	6.6	228	4.986	57	1.614	2	19	18

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		None	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Brandon McCormick	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Brandon McCormick	Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Walter Kenyon		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	William Sanders		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Nathaniel Clague		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Abstain	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Douglas Webb	Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas		Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Terry BIlke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Leanna Lamatrice		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Comments Submitted
3	Clark Public Utilities	Jack Stamper		Abstain	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Brandon McCormick	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Affirmative	N/A
3	Intermountain REA	David Maier		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	Brandon McCormick	Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		Negative	No Comment Submitted
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bryan Taggart	Douglas Webb	Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Affirmative	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	No Comment Submitted
5	City Water, Light and Power of Springfield, IL	Steve Rose		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Abstain	N/A
5	JEA	John Babik		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Comments Submitted
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NaturEner USA, LLC	Eric Smith		Negative	Comments Submitted
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Brett Jacobs		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Abstain	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Mark McDonald		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Vistra Energy	Dan Roethemeyer		Abstain	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Derek Brown	Douglas Webb	Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Nicholas Kirby		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		None	N/A
6	Lakeland Electric	Paul Shipps		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Luminant - Luminant Energy	Kris Butler		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Renee Knarreborg	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	New York Power Authority	Thomas Savin		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	SCANA - South Carolina Electric and Gas Co.	John Folsom		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Grant Wilkerson	Douglas Webb	Affirmative	N/A
6	Western Area Power Administration	Charles Faust		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
7	Luminant Mining Company LLC	Brenda Hampton		Negative	Comments Submitted
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 324 of 324 entries

BALLOT RESULTS

Ballot Name: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 Non-binding Poll AB 2 NB
Voting Start Date: 11/20/2018 12:01:00 AM
Voting End Date: 11/29/2018 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 279
Total Ballot Pool: 300
Quorum: 93
Quorum Established Date: 11/29/2018 1:26:20 PM
Weighted Segment Value: 75.81

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	84	1	44	0.733	16	0.267	20	4
Segment: 2	7	0.6	1	0.1	5	0.5	1	0
Segment: 3	70	1	39	0.796	10	0.204	14	7
Segment: 4	13	1	9	0.818	2	0.182	2	0
Segment: 5	68	1	38	0.776	11	0.224	15	4
Segment: 6	48	1	25	0.781	7	0.219	11	5
Segment: 7	1	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	8	0.7	6	0.6	1	0.1	1	0
Totals:	300	6.4	163	4.704	52	1.696	64	21

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Brandon McCormick	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Louis Guidry	Abstain	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Corn Belt Power Cooperative	larry brusseau		Negative	Comments Submitted
1	Dairyland Power Cooperative	Renee Leidel		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson		Negative	Comments Submitted
1	KAMO Electric Cooperative	Walter Kenyon		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	William Sanders		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	Portland General Electric Co.	Nathaniel Clague		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Abstain	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Douglas Webb	Affirmative	N/A
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas		Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Leanna Lamatrice		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Comments Submitted
3	Clark Public Utilities	Jack Stamper		Abstain	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Brandon McCormick	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Affirmative	N/A
3	Intermountain REA	David Maier		None	N/A
3	JEA	Garry Baker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	Brandon McCormick	Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Joseph Bencomo		None	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		Negative	Comments Submitted
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bryan Taggart	Douglas Webb	Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Abstain	N/A
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		None	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	City Water, Light and Power of Springfield, IL	Steve Rose		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Abstain	N/A
5	JEA	John Babik		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	NaturEner USA, LLC	Eric Smith		Negative	Comments Submitted
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Abstain	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Vistra Energy	Dan Roethemeyer		Abstain	N/A
5	Westar Energy	Derek Brown	Douglas Webb	Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Nicholas Kirby		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		None	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Luminant - Luminant Energy	Kris Butler		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Renee Knarreborg	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	New York Power Authority	Thomas Savin		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Grant Wilkerson	Douglas Webb	Affirmative	N/A
6	Western Area Power Administration	Charles Faust		None	N/A
7	Luminant Mining Company LLC	Amanda Frazier		None	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 300 of 300 entries

Previous 1 Next

Comment Report

Project Name:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | CIP-008-6 (Draft 2)
Comment Period Start Date:	11/15/2018
Comment Period End Date:	11/29/2018
Associated Ballots:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 AB 2 ST

There were 72 sets of responses, including comments from approximately 160 different people from approximately 110 companies representing 7 of the Industry Segments as shown in the table on the following pages.

Questions

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

4. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? Please provide comments and an alternate approach to addressing the directive, if possible.

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

9. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

10, Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO

					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Public Utility District No. 1 of Chelan County	Davis Jelusich	6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC

					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
New York Independent System Operator	Gregory Campoli	2		ISO/RTO Standards Review Committee	Gregory Campoli	NYISO	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Terry BIlke	Midcontinent ISO, Inc.	2	MRO
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Ali Miremadi	CAISO	2	WECC
					Kahtleen Goodman	ISO-NE	2	NPCC
ACES Power Marketing	Jodirah Green	6	NA - Not Applicable	ACES Standard Collaborations	Eric Jensen	Arizona Electric Power Cooperative, Inc	1	WECC
					Bob Solomon	Hoosier Energy Rural Electric	1	SERC

						Cooperative, Inc.		
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3,6	Texas RE
					Chris Bradley	Big Rivers Electric Corporation	1	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Susan Sosbe	Wabash Valley Power Association	3	RF
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aubrey Short	FirstEnergy - FirstEnergy Corporation	4	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Manitoba Hydro	Mike Smith	1		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC

					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC

					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT suggests the SDT consider integrating the two definitions together because there is no longer any purpose in distinguishing between a reportable and non-reportable Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

We are in favor of this change, with the note that, while allowing a Responsible Entity to establish the criteria to define the criteria for an “attempt” it leaves the interpretation of the criteria to be scrutinized by an auditor. Historically, auditors have taken issue with a Responsible Entity’s “definition” and caused issues in audits. In this case, because threat vectors and technology constantly change, and new vulnerabilities are discovered every day, it is difficult and problematic to ask Responsible Entities to define an “attempt.” An auditor could easily take issue with a Responsible Entity’s definition or criteria of an attempted compromise.

The proposed VSL is not reasonable because it creates a greater compliance risk without any reducing cyber risk to the BES. Chasing attempts, documenting attempts, and reporting attempts provides no risk reduction to the BES or BCS. Finding attempts only validates the protections within the CIP standards are working properly. Having to report attempts is just burdensome on RE’s.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
While we agree with the proposed modified definition of Reportable Cyber Security Incidnet, AEP recommends that The phrase “that performs one or more reliability tasks of a functional entity” is redundant to the definition of a BCS and should be struck.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with the proposed modified definitions and with the elimination of ‘reportable attempted cyber security incidents’. BPA appreciates that the SDT recognized entities of varying size face differing threat vectors. BPA supports requiring the Responsible Entity to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light finds that the revised definitions, focused on BES Cyber Systems, add clarity to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Recommend the SDT address/include Physical Security Perimeters in the Reportable Cyber Security Incident definition due to their criticality in relation to BES Cyber Systems and Electronic Security Perimeters.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	

Answer	Yes
Document Name	
Comment	
We agree with the change to include BCS and that PCAs should not be included in the proposed modification to the standard.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
We agree that PCAs should not be in scope.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Comments: No definition provided for the revised terms.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	

Answer	Yes
Document Name	
Comment	
Tacoma Power concurs that PCAs should not be included in the proposed modification to the standard.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

While Dominion Energy supports the revised definitions, we suggest a non-substantive change to add clarity and more closely folow the intent of the SDT.

Dominion Energy recommends the SDT consider adding clarity to the definition of Cyber Security Incident that a compromise or attempts to compromise also only applies to the Electronic Security Perimeter and Physical Security Perimeter. This would make it clear that the first bullet only applies to ESP, PSP, and EACMS associated with High and Medium impact BES Cyber Systems. This would relieve our concern the definition can be misinterpreted and would cause a compromise or attempt to compromise an ESP or PSP as defined in the NERC GOT at a low impact facility would be in scope of the definition. Please consider the proposed alternative language:

Cyber Security Incident:

A malicious act or suspicious event that:

- For High or Medium BES Cyber Systems, compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter, (2) the Physical Security Perimeter, or (3) the Electronic Access Control and Monitoring Systems; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We support the Standards Drafting Team (SDT) modification to Cyber Security Incident and Reportable Cyber Security Incident. Regarding the PCAs as out of scope, Exelon believes it would be beneficial to clarify this out of scope status in the definition of Reportable Cyber Security Incident, which we view as a non-substantive change. Alternatively, Exelon requests clear language in the Implementation Guidance to understand the relationship between the defined terms to avoid confusion and PCAs as out of scope is well documented.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	

EEI appreciates SDT consideration of EEI comments and concerns related to the previously proposed new term, Reportable Attempted Cyber Security Incident and support it's removal. EEI supports the changes made to Requirement R1, parts 1.2.1 and 1.2.2, which address the entity's responsibilities to establish "criteria to evaluate and define attempts to compromise" High and Medium Impact BES Cyber Systems (along with associated EACMS).

We also support the revised definition of "Reportable Cyber Security Incident" as proposed in the current draft.

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE appreciates the drafting team's efforts to resolve the issues identified in the initial ballot. Texas RE agrees with including BES Cyber Systems in the definitions, however, Texas RE recommends revising the proposed definitions to make it clear which types of Cyber Security Incidents must be reported. FERC Order No. 848 specifically directed NERC "to develop and submit Reliability Standard requirements that require responsible entities to report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS" (paragraph 13). Texas RE suggests that the clearest way to do this is to modify the definition of Reportable Cyber Security Incident, since those are the incidents CIP-008 requires responsible entities to submit. It is confusing to have a definition of Reportable Cyber Security Incident, but it not include everything that is reportable. Texas RE request that the SDT place a priority on having total alignment between all these inter-related aspects for the development of this standard.

Texas RE recommends the following definitions:

- Cyber Security Incident
  - A malicious act or suspicious event that compromises, or was an attempt to compromise or disrupt:
    - the Electronic Security Perimeter(s) or
    - Physical Security Perimeter(s) or,

        - Electronic Access Control or Monitoring Systems, or
        - High or Medium Impact BES Cyber System.
- Reportable Cyber Security Incident
    - A Cyber Security Incident that has compromised or was an attempt to compromise, or disrupted:
        - A BES Cyber System; or
        - Electronic Security Perimeter(s); or
        - Electronic Access Control or Monitoring Systems.

· Texas RE recommends changing "*A BES Cyber System that performs one or more reliability tasks of a functional entity*" to BES Cyber System because the former is redundant. The operation of a BES Cyber System would include performing one or more reliability tasks, per CIP-002-5.1a, Guidelines and Technical Basis, BES reliability operating services starting on pages 16/17 and the definition of a BCA, "*A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adverse ly impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems*."

Additionally, Texas RE noticed the Applicable Systems column does not specifically include ESP(s), which means Part 1.2.2 does not specifically include the scenario for Cyber Security Incidents that attempt to compromise a responsible entity's ESP per FERC Order No. 848. While each ESP should have an associated EACMS, the requirement is not clear that attempts to compromise the ESP is included.

This similarly applied to Part 4.2. The Applicable Systems column does not include ESP(s). This could lead to responsible entities not reporting an attempt to compromise an ESP.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy suggests that "that performs one or more reliability tasks of a functional entity" be removed from the Cyber Security Incident definition. This is already contained in the context of CIP-002 and is superfluous.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

As currently proposed, the Reportable Cyber Security Incident (RCSI) definition does not include compromised BES Cyber Systems (BCS) and individual BCS Cyber Assets (BCA).

Cyber Security Incident (CSI) includes only 2 sets:

1. Compromise (or attempt) of ESP, PSP, EACMS
2. Disruption (or attempt) of BCS (implying BCA)

These sets do not include a compromised BCS or BCA. It only includes BCS/BCA that has been disrupted. Therefore, a definition of RCSI that starts with the CSI definition also does not include a compromised BCS or BCA. Likewise, from R1.2, “an identified CSI [… that is] Only an attempt to compromise…” by definition also does not include include an attempt to compromised a BCS or BCA. However, Figures 2 and 3 in the Implementation Guidance suggest that it is intended that compromised BCS are meant to be reported, at least in the attempted case.

It might be argued that a compromised BCA necessarily means the ESP/EACMS was compromised and so the Incident would be reported anyway, but that is not always true. BCAs can be compromised by communication that is legitimately allowed by an ACL or a firewall rule without that EACMS itself being compromised. A real example would be a filesharing protocol allowed by a firewall being used to compromise a Cyber Asset. TCAs and removable media can do the same, even with the CIP mitigating factors in place.

It is suggested that the CSI definition be clarified to include disruption and compromise for all subpoints the way the RCSI definition does.

A second concern is that the defined term “RCSI” does not in fact include all CSI that are reportable as implied by its name. RCSI should be redefined to include all CSI that are in fact reportable, attempted or otherwise. A new, self-evident name, such as Reportable Cyber Attack (RCA), and a corresponding definition should be adopted for RCSI that are determined to be successful attacks, not just mere attempts. The more stringent reporting requirements would then specifically only apply to those RCA.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern greatly appreciates the progress that has been made since draft 1 of the standard. Southern asserts that without additional parameters around the specifics of what constitutes an “Attempt to Compromise” the definitions are painted with too broad a brush. Further defining the terms “Cyber Security Incident” and “Reportable Cyber Security Incident” will allow Registered Entities the opportunity to meet the Standard in a clear and measurable way. Additionally, Southern also agrees with the inclusion of the previously proposed “Reportable Attempted Cyber Security Incident” definition so long as the proper scoping is maintained within the words of the definition. See below for alternative wording for the proposed definitions that clarify the meanings and alleviates ambiguity contained within the current proposed definitions.

Cyber Security Incident – "*an unconfirmed* malicious act or suspicious event *requiring additional investigation to determine if it:*

- For high or medium impact BES Cyber Systems, compromised, or was an attempt to compromise, (1) the ESP, (2) the PSP, or (3) the associated EACMS; or
- Disrupted, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Attempted Cyber Security Incident – "a *confirmed* malicious act that was determined by the Responsible Entity to be:

- An attempt to compromise the ESP of a high or medium impact BCS; or
- An attempt to disrupt the operation of *a high or medium impact* BES Cyber System *or associated EACMS."*

Note: Once confirmed by the Responsible Entity, the incident must be reported within the prescribed timeframes.

Reportable Cyber Security Incident - a *confirmed* malicious act that has:

- Compromised the ESP of a high or medium impact BCS; or
- Disrupted the operation of a BES Cyber System *or high or medium impact-associated EACMS*

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

NRG asserts that the deletion of attachment 1 could cause lack of uniformity of reporting from the industry for meaningful data (i.e. trends in reporting).

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The proposal to include "attempts to compromise" has the potential to expand the scope of the standard to include corporate assets that are not part of a BCS. This increases the burden to entities for increased monitoring and staffing.

Likes 0	

Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	

Comment
Comments: We agree with the commentary provided by NPCC: • Although there seems to be clarity provided by the NERC drafting team that Protected Cyber Assets were not included in the scope of this project, some entities are confused what the expectation is regarding reporting – specifically is the Entity expected to report on PCAs or not? Some entities have indicated that the NERC webinar and guidance contained some conflicting expectations. • There could be a consistency issue with allowing entities to individually define what is an “attempted” Cyber Security Incident is. Further, the exclusion of PCA’s from required reporting poses a limitation to the industry for gathering and disseminating information on potential or actual threats.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The use of two definitions will be confusing to many. In this version, all Cyber Security Incidents are reportable, as specified by Order 848. The term "Reportable Cyber Security Incident" is unnecessary, as it only identifies a level of reporting for one part (Part 4.2) of CIP-008-6. "Reportable Cyber Security Incident" should be removed and replaced with "Cyber Security Incident."

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different. On the proposed definition of Reportable Cyber Security Incident, please clarify that the definition is only associated with the high/medium BES Cyber Systems (BCS).

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment
PCA devices pose a weak link in the protection of the ESP and should be considered for incident reporting.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	No
Document Name	

Comment
Specificity and clarification on “attempt” is needed for the Responbile Entities to establish appropriate critieria for what is expected to be reported.

Likes 0	
Dislikes 0	

Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	No
Document Name	
Comment	
Specificity and clarification on “attempt” is needed for the Responbile Entities to establish appropriate critieria for what is expected to be reported.	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No
Document Name	
Comment	
The proposed changes to the CIP standards being proposed by the SDT for 2016-02 (Virtualization) are proposing terminology changes that will directly impact this language as well as how these changes will be interpreted. Further, the “PCA” (or however they will be referred to) should dbe included. This is because by definition they reside inside the ESP and as such if they are compromised or attempted then the rest of the ESP would be at risk.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.	

On the proposed definition of Reportable Cyber Security Incident, please clarify that the definition is only associated with the high/medium BES Cyber Systems (BCS).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP. Based on last Friday's (November 16) NERC's industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1's Applicable Systems One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	

PPL NERC Registered Affiliates agree that the new definitions are moving in the right direction, however the current definition changes have created inconsistencies.

For example, a Cyber Security Incident does not take a compromise of a BES Cyber System into account when the new Reportable Cyber Security Incident definition specifically requires entities to report on compromised BES Cyber Systems. Therefore, to improve consistency, we would like to suggest the following addition to the Cyber Security Incident definition.

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1) Electronic Security Perimeter, (2) Physical Security Perimeter, or (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems, or
- **Compromises or** disrupts, or was an attempt to **compromise or** disrupt, the operation of a BES Cyber System

Even though Order 848, paragraph 3, does not directly state in the reporting directive that BES Cyber Systems should be included as part of the “Cyber Security Incidents that compromise, or attempt to compromise”, paragraph 19 of the discussion points out that “*unsuccessful attempts to compromise* or disrupt a responsible entity’s core activities are not subject to the current reporting requirements in Reliability Standard CIP-008-5 or elsewhere in the CIP Reliability Standards” (emphasis added). Therefore, we agree with the SDT that it is prudent to include BES Cyber Systems in the definition of Reportable Cyber Security Incident.

We do not agree, however, with the scope of the edits to the definition. We believe that by including BES Cyber System and removing “that perform one or more reliability tasks of a functional entity”, it will accomplish what the SDT has stated was their goal. Therefore, we suggest the following edits to the Reportable Cyber Security Incident definition:

"A Cyber Security Incident that has compromised or disrupted:

A BES Cyber System;

Electronic Security Perimeter(s); or

Electronic Access Control or Monitoring Systems."

Likes 1	ISO New England, Inc., 2, Puscas Michael
Dislikes 0	
Response	

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	

We agree with SDT's decision to NOT create a new proposed term for Reportable Attempted Cyber Security Incident. Thank you for this change from the first posting.

We agree with this posting's proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons.

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

Second. FERC Order 848 directed "NERC to develop and submit modifications to the Reliability Standards 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)." It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: "A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems." This uses language from the FERC Order and is clearer than this proposed posting.

Likes 1	ISO New England, Inc., 2, Puscas Michael
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST recommends that the SDT ELIMINATE the definition of "Reportable Cyber Security Incident." FERC has directed that ALL security events determined to be "Cyber Security Incidents" be reported, which renders the definition of "Reportable Cyber Security Incident" needlessly redundant (and confusing to the casual reader). N&ST believes the different reporting deadlines for attempted vs. actual compromises and/or disruptions can be adequately addressed in Requirement R4. N&ST notes that adopting this recommendation would necessitate minor changes (to eliminate "Reportable Cyber Security Incident") to Requirements R1 through R4. Finally, N&ST strongly recommends that Protected Cyber Assets (PCAs) be considered "Applicable Systems" and included in both the definition of "Cyber Security Incident" and the CIP-008 requirements.

Likes 0	
Dislikes 0	

Response
Brian Evans-Mongeon - Utility Services, Inc. - 4
Answer	No
Document Name	
Comment
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. The Cyber Security Incident Definition speaks to compromise of an ESP but does not include PCAs. Since, by definition, PCAs are inside an ESP, it could be determined that Entities are expected to report on PCAs. We request that the ambiguity be cleared up by explicitly listing PCAs in table R1's Applicable Systems.
Likes 0	
Dislikes 0	
Response
larry brusseau - Corn Belt Power Cooperative - 1
Answer	No
Document Name	
Comment
Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.
Likes 0	
Dislikes 0	
Response
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5
Answer	No
Document Name	
Comment
NV Energy agrees with the SDT's decision to not create a new proposed term for Reportable Attempted Cyber Security Incident. We appreciate the SDT listening to industry comment on this.

NV Energy agrees with this posting's proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

NV Energy would respectively disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons.

- We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

- FERC Order 848 directed "NERC to develop and submit modifications to the Reliability Standards 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)." It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: "A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems." This uses language from the FERC Order and is clearer than this proposed posting.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons:

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

{C}1. definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

Yes

No

Comments: We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons:

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

Second. FERC Order 848 directed, "NERC to develop and submit modifications to the Reliability Standards 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).” It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: “A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems.” This uses language directly from the FERC Order and is clearer than this proposed posting without using excess uneccessary language.

We agree with this posting’s proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

Likes 0	
Dislikes 0	

Response

Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.

Based on last Friday’s (November 16) NERC’s industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1’s Applicable Systems

One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.

Otherwise we agree

Likes 0	
Dislikes 0	

Response

Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle

Answer	No
Document Name	

Comment

We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.

Based on last Friday's (November 16) NERC's industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1's Applicable Systems

One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.

Otherwise we agree

Likes 0	
Dislikes 0	

Response

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

NRG does not have concerns about the Responsible Entities ability to evaluate and define “attempts at compromise” however; NRG asserts that the lack of uniformity in the reporting (i.e. deletion of Attachment 1) could cause difficulty in assessment of the data by E-ISAC and NCCIC, and the resulting conclusions may not be useful to the industry.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

This additional language to R1 Part 1.2 leaves a Responsible Entity’s criteria and definition open to interpretation by an auditor which is concerning.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CenterPoint Energy or Company) agrees with this approach, but would like to note that many events are not attempts or reportable. The Company also requests that the Standard Drafting Team be conscious of including systems that are out of scope as BES Cyber Systems or Electronic Access Control and Monitoring Systems in the Implementation Guidance.

Likes 0	

Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	

Comment
While responsible entities should be encouraged to address this definition of “attempt to compromise or disrupt” related to a Cyber Security Incident, some care should be taken to ensure a minimum level of diligence is expressed in such a definition. A simple form of definition might include documenting judgement of a cyber security analyst at a particular time as the means to determine an attempt (“I’ll know one when I see it”). This may pose some difficulty for auditors trying to assess compliance to this part of the standard. Note: *ERCOT is excluded from the group for this response.*

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
EEI supports the revised language in Requirement R1, Part 1.2; which we believe appropriately places the responsibility for establishing and documenting criteria to evaluate and define attempts to compromise “identified” systems within the responsible entity’s Cyber Security Incident response plan(s). We believe this change will provide entities with the flexibility to tailor criteria in ways that align with their internal processes and procedures to provide clarity and effective reporting.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment

We agree this update allows RE's the ability to establish a solid program.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. The Cyber Security Incident Definition speaks to compromise of an ESP but does not include PCAs. Since, by definition, PCAs are inside an ESP, it could be determined that Entities are expected to report on PCAs. We request that the ambiguity be cleared up by explicitly listing PCAs in table R1's Applicable Systems.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
In addition, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports the intent of the proposed changes. However, we also recognize that Standard still needs and would benefit from guidance on alternative approaches addressing the language,“*establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.”* We are concerned that without established guidance, complying entities and compliance and enforcement staff do not have sufficient guidance to come to common understanding of the draft standard language. Complying public power entities believe that a conservative reporting criteria will present significant costs to administer, without corresponding measurable reliability benefits. The costs required for the follow-up requirements in R4 are significant.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
SDT should consider a minimum criteria for the definition of an “attempt”.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the efforts of the SDT to provide guidance about how an entity might evaluate and define attempts, and finds that guidance sufficient in general.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
These changes are effective when considering how a particular entity can maintain compliance with this standard. Unfortunately, the lack of a universal definition of "attempt" will result in poor data that fails to provide a complete picture of the threat landscape based on attempts across the ERO. A quality standard that addresses both the compliance needs of the industry and the information/data needs of the ERO could have been drafted had the drafting team been given more time and a more thoughtful FERC order.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	Comments for Question 2.docx
Comment	
Please see the attachment for AZPS's response.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
While responsible entities should be encouraged to address this definition of “attempt to compromise or disrupt” related to a Cyber Security Incident, some care should be taken to ensure a minimum level of diligence is expressed in such a definition. A simple form of definition might include documenting judgement of a cyber security analyst at a particular time as the means to determine an attempt (“I’ll know one when I see it”). This may pose some difficulty for auditors trying to assess compliance to this part of the standard.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned that allowing Responsible Entities to establish its own criteria to evaluate and define attempts to compromise (Subpart 1.2.1) will lead to inconsistencies in what is reported which may limit the value of the reported data. Texas RE requests the SDT to define a criteria or reporting threshold for the Cyber Security incidents described in the FERC order. Please see Texas RE's comments in #1 regarding the change to the definition of Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No

Document Name	

Comment

What constitutes an “attempt” should be clearly defined in the standard so that a uniform reporting obligation applies industry-wide. If the purpose of the reporting mandate is to ensure reporting of accurate risk information to E-ISAC and NCCIC for their own analytical purposes and for the purpose of sharing credible threat information with industry, the reporting of that information should be standardized and not left to the judgment of each responsible entity. Furthermore, without a standard definition, responsible entities may be vulnerable to an enforcement determination that the entity’s definition of “attempts” is inadequate. A clear definition helps entities ensure that they are complying with the rule. While the proposed Implementation Guidance is helpful in some respects, it is not obligatory, and therefore leaves open the possibility of a multiplicity of reporting practices. The SDT should consider adopting a list of indicators such as those suggested by the ISO/RTO Council in its comments to FERC in the rulemaking in Docket No. RM18-2.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern has a few concerns with R1, primarily R1.2.1 where the entity must have “One or more processes to establish criteria to evaluate and define attempts to compromise.” We don’t think FERC’s intent for the requirement really is for entities to have a “process to establish criteria.” Entities can establish criteria or have a process to determine whether an event is a true, confirmed attempt to compromise and is reportable, but we don’t think a process to determine the criteria meets the intent of the FERC Order. There is also concern over determining what the possible criteria would be for an attempted compromise. In the absence of a defined term, an attempt that rises to the level of reportability remains very subjective. It would include events that are confirmed as having a malicious intent but aren’t script kiddies or just the normal innocuous noise. It’s not every dropped packet at a firewall but could be some. It’s not every phishing email but could be some. It’s not every failed remote SSH login but could be some. The threshold is going to depend on the facts and circumstances of each event and defies being able to sit down and put into objective and measurable criteria ahead of time. This is why the definitions we have proposed both properly scope reportable incidents as either attempts or actual compromises, and provides the Responsible Entity the levity to make those determinations.

Southern suggests that “establish criteria” be dropped since this problem defies reducing to simple criteria and be replaced by a “process to determine which Cyber Security Incidents should be reported as attempts to compromise.”

Requirement R1.2:

One or more processes to:

1.2.1 Determine if an identified Cyber Security Incident is:

- A Reportable Attempted Cyber Security Incident; or

- A Reportable Cyber Security Incident; and

1.2.2 Provide notification per Requirement R4.

Note: One or more processes to identify, classify, and response to a Cyber Security Incident is already defined as per R1.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy agrees that it is correct for Responsible Entities (RE) to define attempts for their unique programs; however, we are concerned with the language of Requirement R1 1.2. Xcel Energy respectfully suggests removing R1.2.1 in its entirety. R1.1 requires REs to identify Cyber Security Incidents and R1.2.2 requires REs to determine if a Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise. Having an additional enforceable Requirement to establish a set of criteria or methods to evaluate is not needed and is not in the spirit of the Efficiency review project currently under way.

If the Standard Drafting Team choses to go ahead with the language in R1.2.1, Xcel Energy would then suggest that the term “criteria” be removed from the Requirement language. We believe the term "Criteria," is too prescriptive when trying to establish what would be considered an attempt and that a cyber security event that should be reported may not fit into a REs pre-defined set of criterion. We believe that the R1.2.1 should be reworded to read: Have one or more process to: "Establish a documented evaluation method that may include using criteria or other evaluation processes to define attempts to compromise.” This would allow for methods other than a set of prescriptive criteria to evaluate non-conventional events that may not meet established criterion to also be considered as an attempt to compromise but could through some other form of methodology or assessment ultimately be deemed an attempt to compromise. This allows the Requirement language to be flexible enough to ensure entities are able to modify their programs as needed to effectively meet future risks in a changing environment.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

: We disagree with the changes made to Requirement R1, part 1.2.1, which addresses the entity's responsibilities to, "Establish criteria to evaluate **and define** attempts to compromise;"

Recommend remove the term "define," and keep the established scope per NERC, CIP & FERC as: ...

The language would have to be so ubiquitous to cover changes in technologies and encapsulate outlying behavior, that any documented process would be outmoded – and in CONSTANT revisions.

R1.1. already has a criteria to identify the attempts. R.1.1 - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

No - For part 1.2.1, removing "define" allows the entity more flexibility to scope attempts to compromise into their criteria for evaluating the Cyber Security Incident.

R1.2 - One or more processes to: Use: "Respond"?

1.2.1 Establish criteria to evaluate and define attempts to compromise;

1.2.2 Determine if an identified Cyber Security Incident is:

{C}· A Reportable Cyber Security Incident or

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

1.2.3 Provide notification per as specified in Requirement R4 of this Standard.

"**Attempts**" have been a part of the definition for a Cyber Security Incident for more than a decade. PAC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

“Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. NV Energy does not support a process to define “attempts.”

Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for “attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)” in the Reportable Cyber Security Incident definition. Part 1.2 would retain “One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident.” The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to “provide notification per Requirement R4.” This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have not have a reference to reporting.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1

Answer	No
Document Name	

Comment

Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

While the flexibility for entities to define "attempts to compromise” in their unique situations may be desirable, guidance should be provided outlining the characteristics common to these attempts.

Likes 0	

Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
If the SDT deems it important to add an explicit requirement to define and document criteria for identifying Cyber Security Incidents (it's already implied by the language of existing CIP-008 R1 Part 1.1), N&ST believes it should be added to R1 Part 1.1, not R1 Part 1.2. N&ST also recommends changes to the proposed of language of R1 Part 1.2.2. Per FERC's directive, all Cyber Security Incidents are to be considered "reportable" (N&ST also recommends eliminating the definition of "Reportable Cyber Security Incident," as per our response to Question 1). N&ST agrees that an actual compromise of an ESP or an applicable system should be distinguished from an (unsuccessful) attempt but objects to the use of the word, "only" (as in "Only an attempt..."), as it implies triviality. Suggested re-wording: "Determine whether an identified Cyber Security Incident was an attempt to compromise an ESP or an applicable system or actually compromised or disrupted an ESP or an applicable system."

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	

Comment
"Attempts" have been a part of the definition for a Cyber Security Incident for more than a decade. MEC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted. Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting. Additionally, we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3 With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
LES has ongoing concerns about the lack of a clear and concise definition for “attempt to compromise”, but does understand the challenge of creating a one size fits all definition. The guidance document developed by the drafting team provides good examples of what does and what does not constitute an attempt to compromise.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
The lack of any guidance for industry to review makes it very difficult for us to provide a more productive set of comments. It would be very helpful if additional specifics on what would justify as an “attempt to compromise” were provided in guidance, which would reduce confusion during a regulatory engagement.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

Comments: Further clarification on what qualifies as an attempt to compromise a system, and a definition of “attempt” are needed.

Likes 0	
Dislikes 0	

Response

Seth Shoemaker - Muscatine Power and Water - 3

Answer	No
Document Name	

Comment

While having the flexibilty to establish and document our own criteria may be beneficial, we believe this leaves too much room for interpretation and may not address the security objectives of the Standard if an entity chooses not to include specific criteria in their plans. Additionally, because entities will establish and document independent criteria, this creates room for auditors to determine their preferred criteria and attempt to hold entities to that Standard. We recommend the SDT establish and document minimum required criteria to evaluate and define attempts to compromise to create a baseline for entities to be held to.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - 1

Answer	No
Document Name	

Comment
While it is makes sense that each Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems, there is some concern on the auditablility of such a requirement. There is concern that without a more clear objective in the requirement, a Responsible Entity may have implemented, in good faith, a criteria to evaluate and define an attempt to compromise; however, an auditor may not agree, thus resulting in a potential instance of noncompliance.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No
Document Name	

Comment
One of the four elements outlined by FERC was to improve the quality of reporting and allow for ease of comparison. In order to collect consistent data across all Responsible Entities it is necessary to provide specificity to “attempt”.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No

Document Name	

Comment

Part 1.2 is unnecessary and duplicative of Part 1.1. The language of Part 1.2.1 and Part 1.2.2 describes some parts of the classification of a Cyber Security Incident, which is required by Part 1.1. Part 1.2.3 specifies notification, which is part of response required by Part 1.1. Any language needed to clarify the basic requirements of "identify, classify, and respond" should be included in Part 1.1, not a separate Part.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

: If the satandard as written is approved, then Responsible Entities should be allowed to define attempts based on their environment configuration, however, the proposal to include "attempts to compromise" has the potential to expand the scope of the standard to include corporate assets that are not part of a BCS. This increases the burden to entities for increased documentation of attempts.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	No
Document Name	

Comment

AEP believes if all the RE’s have their own criteria to evaluate and define then Responsible Entities run the risk of reporting (or not reporting) different incidents. While it is challenging to come up with a common definition of a reportable incident, consistency is needed to ensure the appropriate CSI’s are reported to satisfy FERC Order 848.

Likes 0	
Dislikes 0	

Response

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

In R1.2.2 the term “only” is introduced in the Requirement language, in the Measures, and is also used in the Requirement language of R4.2. Xcel Energy believes that the use of the term “only” may create a situation in which a Responsible Entity (RE) would need to prove to an auditor that an event was in fact “only” an attempted event and not an actual compromise. This would put a RE in a position where they would need to prove the negative. By removing “only” from the Standard language it will remove the implication that a RE has made that permanent determination that it was an attempt. The removal of “only” will not substantively change the intent of the Requirement. We see this as an important change to ensure that attempts to compromise are promptly reported while still allowing on-going monitoring and evaluations to determine if an actual compromise has occurred which in some cases could be some time in the future.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Please note that even though the NSRF agrees with our flexibility to establish our own criteria, we believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criterias of what an attempt to compromise is.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light finds the changes clarifying, and finds the additional guidance helpful in developing an acceptable process to determine what is an attempt to compromise.	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
An entity's processes for Part 1.2 should include establishing criteria to evaluate incidents (Part 1.2.1), determine if Cyber Security Incidents are Reportable or an attempt (Part 1.2.2), and how to provide R4 notifications including each Part of R4 (Part 1.2.3). Thus, the entity's Part 1.2 process(es) must address *what* is included in initial notifications (Part 4.1), when they are to be submitted after determinations (Part 4.2), and how to provide updates as determined with new or changed attribute information within 7 days (Part 4.3). Consequently, the entity's determination utilizing the Part 1.2 process should lead to initial notifications outlined in Part 4.2.	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Referring to the “Applicable Systems” column in the “Requirements” column may be redundant. A suggestion for the language in the second bullet for Part 1.2.2 is: “An attempt to compromise (as defined in Part 1.2.1) one or more applicable systems.”	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
However, guidance from the SDT would be appreciated to set a baseline for what an attempt to compromise is to ensure consistent application of the requirements.	

Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Tacoma Power believes that the proposed changes reflect that an Entity must have a process in place identify compromise attempts and provide notification. Tacoma Power is concerned that specifying a specific number of days for reporting actual and attempted Cyber Security Incidents to agencies will sometimes be a resource challenge. Tacoma Power recommends that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1. Physically getting a team to remote substations to determine the attack vector could take time and difficulty will be increased depending the how wide-spread the event turns out to be.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI believes the proposed language clearly defines that responsible entities must have processes in place within their Cyber Security Incident Response plans that determine what an attempt to compromise is along with their reporting responsibilities. Although we support the revised language in Requirement R1 Part 1.2 and Requirement R4 Part 4.2, we suggest the SDT consider making the following minor modification to the phrase “only an attempt to compromise” to “an attempt to compromise”. (see Subpart 1.2.2, Measures for Part 1.2, Measures 2.3 and Requirement R4) Although we understand the SDT’s reasoning for adding “only” to the phrase, we believe it offers little additional clarity yet does have the potential for adding confusion to the phrase. Moreover, within Requirement 1, Subpart 1.2.1 entities are clearly required to define “attempts to compromise”.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

The changes do clarify that responsible entities must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2. However, please see Texas RE's concern with Responsible Entities developing their own processes in #2.

Given Texas RE's proposed changes to the definitions as described in #1, the reporting timelines in Part 4.2 should be changed to:

-
  - One hour after the determination of a Cyber Security Incident that compromised or disrupted
    - Electronic Access Control or Monitoring Systems.
    - Electronic Security Perimeter(s); or
    - A BES Cyber System; or
  - By the end of the next calendar day after determination of a Cyber Security Incident that **was an attempt to compromise** or disrupt:
    - Electronic Security Perimeter(s); or
    - A BES Cyber System; or

- Electronic Access Control or Monitoring Systems.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Please see our response to Question 1. We agree with the concept, but it will require further definition of key terms detailed above to allow Registered Entities the opportunity to meet the Standard in a clear and measurable way.

As for the language of R4, itself, Southern Company suggests the following edits to clarify the scope and applicability that is based on the revised definitions proposed under Q1:

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)1, or their successors, of a Reportable Attempted Cyber Security Incident ***or*** *a Reportable Cyber Security Incident.*

For Section 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:

- By the end of the next calendar day after determination of a *Reportable Attempted Cyber Security Incident.*
- One hour after the determination of a Reportable Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Part 4.2 stands on its own. Notification is part of "respond" in Part 1.1 and does not need Part 1.2. Part 4.2 should be clarified so show that all events that meet the definition of "Cyber Security Incident" are reportable, but that only actual compromise or disruption is reportable within one hour.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

Comments: Request clarifications on the measures and evidence needed to satisfy the requirement.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

See previous comment.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

“Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. MEC will not support a process to define “attempts.” Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain.

Further, see the last question for comments on Requirement 4 and its Parts. There are not questions for Requirement 4 in this comment form.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
N&ST agrees that an actual compromise of an ESP or an applicable system should be distinguished from an (unsuccessful) attempt and that it is reasonable to define different reporting time frames for each type of Cyber Security Incident. However, N&ST objects to the use of the word, “only” (as in “Only an attempt...”), as it implies triviality (N&ST also recommends eliminating the definition of “Reportable Cyber Security Incident” as per our response to Question 1). Suggested re-wording for R1 Part 1.2: “Determine whether an identified Cyber Security Incident was an attempt to compromise an ESP or an applicable system or actually compromised or disrupted an ESP or an applicable system.” Suggested re-wording for R4 Part 4.2 “bullets:” (1st) “One hour after a determination that a Cyber Security Incident was an actual compromise or disruption of an ESP or an applicable system.” (2nd) “By the end of the next calendar day after a determination that a Cyber Security Incident was an unsuccessful attempt to compromise or disrupt an ESP or an applicable system.”	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy would like to reiterate that “Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. NV Energy does not support a process to define “attempts.” Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain.	
Likes 0	

Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment

: We disagree with the changes made to Requirement R1, part 1.2.1, which addresses the entity's responsibilities to, "Establish criteria to evaluate **and define** attempts to compromise;"

Recommend remove the term "define," and keep the established scope per NERC, CIP & FERC as: ...

The language would have to be so ubiquitous to cover changes in technologies and encapsulate outlying behavior, that any documented process would be outmoded – and in CONSTANT revisions.

R1.1. already has a criteria to identify the attempts. R.1.1 - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

No - For part 1.2.1, removing "define" allows the entity more flexibility to scope attempts to compromise into their criteria for evaluating the Cyber Security Incident.

R1.2 - One or more processes to: Use: "Respond"?

1.2.1 Establish criteria to evaluate and define attempts to compromise;

1.2.2 Determine if an identified Cyber Security Incident is:

{C}· A Reportable Cyber Security Incident or

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

1.2.3 Provide notification per as specified in Requirement R4 of this Standard.

"**Attempts**" have been a part of the definition for a Cyber Security Incident for more than a decade. PAC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's

Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

{C}1. Do the changes clarify that the Responsible Entity **must have a process to determine** what is an **attempt** to compromise and provide notification as stated **in Requirement R1 Part 1.2 and Requirement R4 Part 4.2**? Please explain and provide comments.

{C}{C}{C} Yes

{C}{C} No

Comments: We disagree that the changes clearly, or need to clarify, based on the following;

R1.1 lays out the criteria to identify Cyber Security Incidents (***which by definition includes attempts***) - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

They include compromises and attempts to compromise. Remove the language, "**and define**…" as stated in: 1.2.1 Establish criteria to evaluate **and define** attempts to compromise; The requirement as stated is too restrictive and would require too many itemizations and feverish revisions as methods and technolies are developed. – uggest to utilize the term and process of 'evaluation' as stated in the R.1. : " identify, classify, and respond" measures. Recommend removal of R.1.2.1, and stick with R.1.1. The scope and intent are included in R.1.1.

PAC will not support a process to define "attempts." **Industry has been identifying attempts for years.** Part 1.2 should be changed to accomplish the FERC directive, and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms, or Parts, creates additional work for Entity's to revise, implement and retrain.

Further, see question #10, for comments on Requirement 4, and its Parts. **There are not questions for Requirement 4 in this comment form**:

There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, R4 only needs to refer to Reportable Cyber Security Incidents. It does not need to include "a Cyber Security Indicent that was only an attempt to compromise a system identified in the "Applicable Systems" column. This phrase could be deleted.

Suggest change to the following:

"was only an attempt to compromise an identified system applicable system identified in the "Applicable Systems" column for this Part." As identified in R.1.2.2:

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

Review for redundancies: These are defined in scope in the 'Applicable Systems' in Column One of the Standard.

Likes 0	
Dislikes 0	

Response

4. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? Please provide comments and an alternate approach to addressing the directive, if possible.

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy agrees with the addition of EACMS to the Applicable Systems. Additionally, the Company suggest that entities be allowed to restrict indications of compromise or attempt to compromise to the capability of the EACMS.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

FERC Order 848, ¶ 54 states, “With regard to identifying EACMS for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide.” We agree with adding “and their associated” EACMS” to the Applicable Systems columns in the Parts. We thank SDT for ensuring these changes keep low impact out of scope for reporting.

Likes 0	
Dislikes 0	

Response

Renee Leidel - Dairyland Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Yes, but I think it should be further qualified to only those systems involved in controlling access. EACMS currently includes systems that may only be for monitoring security that Project 2016-02 would classifiy as EAMS. It seems the intention of adding “EACMS” to the standard here is to target

reporting of what Project 2016-02 calls “EACS” systems. Will this new requirement unqualified be a barrier to utilizing external services related to monitoring access?	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Adding EACMS as CIP-008 applicable makes sense to improve the BES security posture. If the systems controlling access and monitoring a BCS are under attack, response and notification should be required.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	

We agree with adding “and their associated” EACMS” to the Applicable Systems columns in the Parts. We thank SDT for ensuring these changes keep low impact out of scope for reporting.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	Yes
Document Name	

Comment

LES anticipates this matter will be "cleaned up" in the virtualization project, within this project the SDT is proposing to seperate EACMS into EACS and EAMS.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

In addition, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Tommy Drea - Dairyland Power Cooperative - 5

Answer	Yes
Document Name	

Comment

Yes, but I think it should be further qualified to only those systems involved in controlling access. EACMS currently includes systems that may only be for monitoring security that Project 2016-02 would classifiy as EAMS. It seems the intention of adding “EACMS” to the standard here is to target reporting of what Project 2016-02 calls “EACS” systems. Will this new requirement unqualified be a barrier to utilizing external services related to monitoring access?

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light understands the difficulty faced by the SDT regarding EACMS and FERC Order No. 848. We cannot identify a better alternative and reluctantly agree with the proposed approach.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to #1 regarding including ESPs as applicable systems.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern asserts that the language, as proposed, DOES extend the scope into CIP-003 and low impact BES Cyber Systems. The currently approved definition of "Reportable Cyber Security Incident" has a threshold of actually compromising or disrupting a reliability task of the functional entity. With the SDT's proposed changes to the definition and its use in CIP-003, what is reportable at assets containing lows could now be any compromise or disruption of any BES Cyber System, any "logical borders surrounding a network to which BES Cyber Systems are connected using a routable protocol", any "physical borders in which BES Cyber Assets reside…" or any EACMS. It appears the SDT attempts to limit the CIP-003 scope expansion with the use of the nested "Cyber Security Incident" definition. The EACMS are scoped to high and medium in the CSI definition and then uses it as the basis of the Reportable CSI definition. Southern asserts that the ESP (and PSP) term in the CSI definition is not likewise scoped and leaves an ambiguity. Simply because no requirements in CIP-005 or CIP-006 apply at a site that only contains low impact systems does not mean that a logical or a physical border does not exist at the location that meets these definitions. Therefore, if a firewall at a 100kV "low only" substation is plugged into a UPS and the UPS "suspiciously" powers off, then both an ESP (the logical border…) and an EACMS is disrupted at that low	

substation. It seems to be reportable under one sub-bullet (ESP) but not another (EACMS) and therefore becomes a reportable incident under CIP-003 (CIP-008's scoping language has no bearing on this situation).

Southern suggests this ambiguity can be removed by moving the qualifier for high and medium to earlier in the definition, as suggested under Southern's proposed modifications presented in Q1, and by also specifying high and medium impact-associated EACMS under the Reportable Cyber Security Incident definition:

Cyber Security Incident – *an unconfirmed* malicious act or suspicious event *requiring additional investigation to determine if it:*

- For high or medium impact BES Cyber Systems, compromised, or was an attempt to compromise, (1) the ESP, (2) the PSP, or (3) the associated EACMS; or
- Disrupted, or was an attempt to disrupt, the operation of a BES Cyber System

Reportable Attempted Cyber Security Incident – a *confirmed* malicious act that was determined by the Responsible Entity to be:

- An attempt to compromise the ESP of a high or medium impact BCS; or
- An attempt to disrupt the operation of *a high or medium impact* BES Cyber System *or associated EACMS.*

Note: Once confirmed by the Responsible Entity, the incident must be reported within the prescribed timeframes.

Reportable Cyber Security Incident – a *confirmed* malicious act that has:

- Compromised the ESP of a high or medium impact BCS; or
- Disrupted the operation of a BES Cyber System, *or high or medium impact-associated EACMS*

In fact, Southern suggests that "Electronic Security Perimeter" could be deleted from the definition now that EACMS has been added, as the two appear redundant. Would not any attempt to compromise or disrupt "the logical border…" occur at an EACMS? Southern provides this as a point of discussion only.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

EACMS should not be included. Systems that only perform the 'Monitoring' portion of an EACMS should not be included due to the minimal risk they pose compromising the BES. TVA has taken an enterprise approach to Cybersecurity monitoring and the system is implemented and designed to be isolated from the BES components in such a manner that a compromise of the system can in no way impact the BES.

Likes 0	
Dislikes 0	

Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No
Document Name	
Comment	
I marked No here because of my comments in question 1 above. Those thoughts regarding the SDT 2016-002 are applicable here as well.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
POPUD is afraid that the way this is addressed will cause ambiguity and confusion for low impact BES Cyber Systems, and unnecessary reporting of minor issues invoving low impact assets.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole does not agree with the inclusion of EACMs.	
Likes 0	
Dislikes 0	
Response	

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy believes that additional clarity should be provided in Requirement 4.2 so that it is stated that notifications of a Reportable Cyber Security Incident must be made one hour after its determination, even if it was already reported as an attempt. The upgrade from an attempt to an actual compromise requires a new notification within 24 hours per Requirement 4.2, not just an update.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company supports the “update timeframe” in R4.4 to be set at 7 calendar days which will facilitate regular and timely reporting for issues of an extended duration. This timeframe will facilitate the ability for a registered entity who experiences a need to update attribute information to do so on a regular weekly schedule until all attributes have been reported.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

Likes 0	

Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
While AZPS appreciates the change from 5 to 7 calendar days, as noted in our previous comments, a continual updating of information every 7 days may result in inaccurate information and an undue burden on resources. Therefore, it is recommended that an initial notification is made and then a final update at the completion of a Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments. Aditionally, while WEC Energy Group supports the proposed reporting timeframes, we recognize the need for a CIP Exceptional Circumstances clause to be added to Requirement R4 to manage the situation where the reporting timeframe cannot be met due to declared CEC.	
Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the additional time allowed for follow-on reporting, which better accommodates uncommon situations that, nonetheless, occur with some regularity, such as holiday season, vacations, and operational emergencies.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
We appreciate that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement may add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	

We appreciate that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement may add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits

Likes 0	
Dislikes 0	

Response

Matthew Beilfuss - WEC Energy Group, Inc. - 4

Answer	Yes
Document Name	

Comment

While WEC Energy Group supports the proposed reporting timeframes, we recognize the need for a CIP Exceptional Circumstances clause to be added to Requirement R4 to manage the situation where the reporting timeframe cannot be met due to declared CEC.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - 1

Answer	Yes
Document Name	

Comment

Referring to the “Applicable Systems” column in the “Requirements” column may be redundant. A suggestion for the language in the second bullet for Part 4.2 is: “By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise (as defined in Part 1.2.1) one or more applicable systems.”

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Yes we agree 7 is more suitable timeframe because it allows the organization to be more thorough in analysis performance, evidence gathering and fact finding, before reporting back to the region.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy agrees with the additional days for reporting additional information to E-ISAC and NCCIC.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

There should be a consistent reporting timeframe for all, R4.2 & R4.3. A SEVEN calendar day reporting timeframe allows an entity a more reasonable timeframe to report, and subsuqent follow-up reporting. FERC Order 848, ¶ 53 states, "…NERC should have the flexibility to establish an appropriate reporting threshold." This increase supports this.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

ERCOT requests that CIP Exceptional Circumstances be added to Part 4.2. As ERCOT noted in its comments on the last version, responsible entities need to focus on reliability and restoration without the burden of meeting a reporting deadline during these activities. Alternatively, this could be added to the overarching Requirement R4. In the SDT's consideration of comments for the last version, the SDT noted that the 2016-02 SDT would address this. ERCOT requests that the 2018-02 SDT address this in in the new requirement being developed since the new reporting timelines will be subject to the implementation plan for CIP-008-6. Proposed language: Part 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, except during CIP Exceptional Circumstances:".

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

While we agree with the increase in the reporting timeframe from 5 to 7 calendar days in Part 4.3, we still have concerns with the reporting timeframes in Part 4.2. We strongly encourage NERC and the SDT to reconsider requiring each Responsible Entity (RE) to report to two different agencies (E-ISAC and NCCIC). If NERC cannot coordinate with both agencies to have one central reporting mechanism, we would recommend expanding the timeframe to allow for one hour per agency, which would change the Part 4.2 requirement to: *"**Two hours** after the determination of a Reportable Cyber Security Incident. **48 hours** after determination that a Cyber Security Incident was only an attempt..."* Rationale behind this suggestion can be illustrated with the following example: If an RE decides to contact the E-ISAC as the first agency and makes a phone call for initial notification, but is placed on hold for an extended time, it is possible that reporting to the NCCIC (as the second agency) may fall outside of the one hour window. We believe that by doubling the reporting agencies, REs should receive double the amount of time to report, especially in times of crisis when there may be longer delays/higher volume in contacting these agencies. This updated requirement is doubling the reporting requirements of CIP-008-5 while keeping the same one hour reporting timeframe for Reportable Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulations have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.	
Likes 0	
Dislikes 0	
Response	

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	
Tacoma Power appreciates that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement will add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits.	
Likes 0	
Dislikes 0	
Response	

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.	
Likes 0	

Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the timeframes are confusing and could result in unintended actions such as shortened investigations and minimal reporting. Requirements with timeframes are often most violated unintentionally. This could especially be the case during a high-stress incident response scenario. Suspicious system behavior could take a long time to understand and resolve. Entities should not be penalized for not reporting new information gained over a long timeframe.	
Likes 0	
Dislikes 0	
Response	

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company notes that the CIP-008-6 Standard language has changed for notification methods, yet the Technical Rationale, in the section labeled "**Methods for Submitting Notifications",** references "submit notification using any *approved* method supported by E-ISAC and NCCIC". Southern Company requests that this be changed to read, "submit notification using any method supported by E-ISAC and NCCIC." The use of "approved" implies an approval process that is not addressed in the current Standard language or draft Implementation Guidance.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	

Comment

While we agree with the SDT's decision to provide flexibility in notification methods, with regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three agencies during initial and updated submissions. If automation is not possible, consider adding a check box on the form indicating that E-ISAC needs to forward the report to NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency's form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE's responsibility to report to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."

- In addition, in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful*

government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy wants to commend the SDT for listening to industry comment and removing the form for communication, and allowing Entities the flexibility to determine notification. We would also request that any upcoming drafts not include this Appendix.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the SDT's decision to provide responsible entities the flexibility to determine the most effective notification method for submitting Cyber Security Incident information to the E-ISAC and ICS-CERT within their processes.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST supports giving Responsible Entities this flexibility but is concerned about the possibility that the recipients of these notifications may be unwilling to accommodate a multitude of different notification methods and report formats. N&ST recommends that NERC, the Regions, the E-ISAC and the DHS work cooperatively to define a SINGLE report template that can be used system-wide to reduce administrative overhead.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	

Comment	
We thank the SDT for responding to comments and eliminating the proposed appendix in the standard. Do not put it back in the standard.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
The flexibility that this change provides will allow entities to modify reporting formats as technology, regulatory requirements, and possibly organizations being reported to change over time.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Recommend the SDT consider the addition of identifying potential notification methods to the Part 1.2 measures to ensure these details are not overlooked when entities develope processes.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light generally is agnostic to reporting method, but would prefer that if duplicate reporting is required, both reports can be made by the same method and format. See also discussion in question 9.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
It is not clear how auditors, or enforcement staff, will be restrained from exercising subjective judgement of sufficiency regarding the entites' notification methods and process.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No

Document Name	
Comment	
I am not sure of the rationale behind removing 4.2 from the standard. It seemed to cover nearly any type of method of notification. So if by that it is intended to provide flexibility I guess that the notification process should be required to be noted as part of the plan so that it can be traced in the event of an incident.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	
It is not clear what the SDT means with the language, "*flexibility to determine notification methods in their process.*" Is this referring to language in the R 4.2 that was deleted in this version? Otherwise, the "flexibility" is not included. The measures for the new R 4.2 state just a single measure: *Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC*.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
Comments: There should be a standardized reporting form which gathers all required attributes and necessary information that is automatically sent to multiple agencies once submitted (e.g single portal which distributes to E-ISAC and NCCIC).	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	

Answer	No
Document Name	
Comment	
One of the four elements outlined by FERC was to improve the quality of reporting and allow for ease of comparison. In order to collect consistent data a framework for reporting is needed.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	No
Document Name	
Comment	
We are unsure what the SDT considers the “flexibility to determine notification methods in their process”. Is this referring to language in the 4.2 that was deleted in this version? Otherwise, we do not see flexibility included. The measures for the new 4.2 state just a single measure: Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	

Answer	No
Document Name	
Comment	
Comments: A formal template should be provided to industry to ensure consistent information is provided.	
Likes 0	
Dislikes 0	
Response	

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the additional time allowed to develop, implement, and socialize the revised incident response and reporting requirements.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
What is the SDT's intent for the initial performance of Part 2.1? Recommend the SDT address Part 2.1 in the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
We support the extended implementation timeframe.	
Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
We support the extended implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST supports this change. N&ST believes it may require considerable amounts of time and effort for Responsible Entities to define, test and, as necessary, adjust criteria and metrics that they will use to distinguish “noise” from serious attempts to compromise their operational cyber infrastructures. It may also take considerable amounts of time and effort to define and, in some instances, assign staff to reporting functions.	
Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We agree with the adjusted 18 month timeframe as it was necessary to assist RE's in setting up its documented approach for classifying and reporting attempts. The time is also needed to adjust internal processes, provide training to necessary staff, and implement the changes to reporting.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the SDT’s decision to move to an 18-month Implementation Plan in response to Industry comments.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The additional time for implementation is well needed given the additional administrative burden on Entitie's to meet this Reliability Standard.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company believes that due to the program changes required, 24 months is necessary. Given that these changes go from reporting known, clearly defined, objective events that have caused actual impact, to a very subjective “attempts to compromise” that are not easily and quickly determined, nor lend themselves to automated detection without flooding the intended recipients, it will require Responsible Entities to deploy additional resources, modify many existing security processes, potentially implement additional security controls and systems, and coordinate these changes across large enterprises. Therefore, 24 months is a more reasonable timeframe for successful implementation of the necessary changes.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

For small to medium sized RE's, a significant lift is required to staff the required positions, train/retrain, implement the technologies and create cross functional processes to meet the newly revised standards. A 24 month Implementation Plan is recommended.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel appropriately.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tommy Drea - Dairyland Power Cooperative - 5

Answer	No
Document Name	

Comment

These changes should not be a significant effort to implement and 12 months seem sufficient to update program documentation and train SMEs of the changes. This standard would need to be revised again if Project 2016-02 is implemented and the definition for EACMS changes. If the implementation timeline is extended too far, a conflict could add more work.	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	No
Document Name	
Comment	
These changes should not be a significant effort to implement and 12 months seem sufficient to update program documentation and train SMEs of the changes. This standard would need to be revised again if Project 2016-02 is implemented and the definition for EACMS changes. If the implementation timeline is extended too far, a conflict could add more work.	
Likes 0	
Dislikes 0	
Response	

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

While EEI generally agrees with the Violation Severity Levels, we suggest the SDT consider making the following minor modification to the phrase “only an attempt to compromise” to “an attempt to compromise”. Although we understand the SDT’s reasoning for adding “only” to the phrase, we believe it offer little additional clarity yet does have the potential of adding confusion to the phrase. Moreover, within Requirement 1, Subpart 1.2.1 entities are required to define “attempts to compromise”.

Affected VSL:

- R1, Severe VSL
- R2, Severe VSL
- R4, Lower VSL, Moderate VSL

Likes 0	
Dislikes 0	

Response

Renee Leidel - Dairyland Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Generally yes, but R4 appears to have an error. The same text “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident (R4)” appears under both High VSL and Severe VSL columns.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Generally yes, but R4 appears to have an error. The same text “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident (R4)” appears under both High VSL and Severe VSL columns.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA thanks the SDT for making the modifications.	

Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Due to shorted balloting period Xcel Energy was not able to evaluate the modifications to VRF or VSLs.	
Likes 0	
Dislikes 0	

Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
No opinion.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
As stated above, any auditor can take issue with a Responsible Entity's "criteria to evaluate and define attempts to compromise" as it is impossible to define with ever changing threats. Because an auditor can interpret this, a High VSL to R1 is not reasonable. We recommend low and moderate for "attempts".	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company does not support the VRFs and VSLs for Requirement R1 and R4 and consider that they do not appropriately outline the true minimal risk and potential severity to the BES, as written. Given the risk-based nature of NERC's CMEP program, Southern requests the addition of Lower and Moderate VSLs under Requirement R1, and language detailing truly tiered severity levels. Examples for Requirement R1: Lower VLS:	

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2)

Moderate VSL:

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Attempted Cyber Security Incidents.

High VLS:

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents.

Examples for Requirement R4:

Lower VLS:

The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

For R1, we believe that failure to include processes to identify Cyber Security Incidents that were only an attempt to compromise an applicable system should be at a lower VSL than failing to include processes to identify Reportable Cyber Security Incidents (RCSI) as there is a clear difference in a RCSI's potential impact to the BES versus only an attempt (which would not have an actual impact to the BES). We believe that all failures related only to attempts should be classified as "Lower VSL" based on their lack of actual impact to the BES. Similarly, for R4, the same logic should apply. A failure to notify an information sharing organization of an unsuccessful attempted Cyber Security Incident should not result in a Moderate VSL, but rather a Lower VSL based on actual impact to the BES (or lack thereof). Furthermore, if a Responsible Entity only notified one agency, this should be considered nothing higher than a Lower VSL as the incident was still reported and should have been shared between agencies.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee

Answer	No

Document Name	
Comment	
For R4, there seems to be duplication of criteria for Severe and High VSL regarding the following: “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4).” Which shows up in both columns (Severe and High VSL). Otherwise, the VSL language seems appropriate.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Given our comments on previous items, NV Energy cannot approve the currently drafted VRF and VSLs, as our comments on revisions would require changes be made to the VRFs and VSLs to reflect NV Energy's recommendations.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	

Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
We do not agree with Requirements and Parts as proposed. The VRFs and VSLs have to be revised too.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
The current proposed requirements still need to be refined by the Standard Drafting Team. And the VRF and VSL should be updated accordingly.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment	
While we don't agree, we have found it doesn't merit the effort to provide alternatives.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
The current proposed requirements still need to be refined by the Standard Drafting Team. And the VRF and VSL should be updated accordingly.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
Comments: Until the standard language is more formalized the Violation Risk Factors or Violation Severity Levels may not accurately reflect the risks.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

For R4, there seems to be duplication of criteria for Severe and High VSL regarding the following:

“The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4).”

Which shows up in both columns (Severe and High VSL).

Otherwise, the VSL language seems appropriate.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation does not agree with the High VSL for R4. Reclamation recommends changing the High VSL

from:

The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3.

to:

The Responsible Entity notified E-ISAC and DHS, or their successors, but did not accomplish the initial notification within the timeframes included in Requirement R4 Part 4.3.

Reclamation also recommends adding the following as a third option to the Moderate VSL:

The Responsible Entity initially notified E-ISAC and DHS, or their successors, within the timeframes included in Requirement R4 Part 4.3 but failed to update E-ISAC or DHS, or their successors, within the timeframe included in Requirement R4 Part 4.4.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment
R1 Severe VSL seems to be extreme for an admisitrative failure to include "only and attempt to compromise". R1 High VSL seems to be extreem for the administrave failure to have a process to identify criteria to define attempts to compromise. POPUD forsees arguments between the entity the auditors and enforcement staff over the sufficiency of these sections. We are aware of instances where auditors have decided that an issue was techicallyaddressed, but it wasn't addressed to their satisfaction. Most recently there is a discussion of the sufficiency of certain chains and locks used for CIP-014. We would like these issues addressed going forward during Standard development, rather than when the Standards are being enforced.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful attempted Cyber Security Incident should not result in a severe penalty.

Likes 0	
Dislikes 0	

Response

9. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

NRG does not have concerns in acheiving these reliability objectives in a cost effective manner; however, this may be challenging for Responsible Entities who have manual processes for evaluation.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

However, the auditors may not agree with the cost effective approach and demand a higher level (best practices) application. This puts smaller entities in jeopardy during audits.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We appreciate the development of the Implementation Guide and we agree with SDT approach to allow RE's to develop a model based on the analaysis of the current environment and the time to discuss future projections for realistic budgetary stance.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	

Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

While we generally agree with the SDT's modifications to provide flexibility, with regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three agencies during initial and updated submissions. If automation is not possible, consider adding a check box on the form indicating that E-ISAC needs to forward the report to NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency's form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE's responsibility to report to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."

- In addition in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government*."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

The new standard ultimately requires Responsible Entities to become cyber security threat hunters rather than relying on the protections required within the CIP standards. There is no reduction in risk to the BES in reporting attempts to compromise. CIP-008-6's new requirements are going to require significant investments in technology and personnel for small and medium sized Regional Entities without an existing 24x7x365 Security Operations Center (SOC). A 24x7x365 SOC, is a multi-million dollar capital investment and a significant operational and maintenance budget burden. At a minimum, a SOC requires six qualified FTE to cover shifts plus, a threat hunter, oversight, compliance reporting, and management. Salaries alone for a small SOC are in excess of $1,000,000. This is just not feasible for a small or medium sized entity. Using a Managed Service Provider for SOC services to reduce cost is also not feasible due to access to BCSI, its inherent requirements, and increased compliance risk.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Including EACMs increases documentation of attempts which makes the requirement onerous for the entities.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Prior to proposing additional modifications, Reclamation recommends each SDT take the necessary time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities with economic relief by allowing technical compliance with current standards.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

With regard to reporting to two independent agencies (E-ISAC and NCCIC), it seems strange to have duplicate reporting. Would it not make sense to avoid such inefficiency by simply reporting to E-ISAC and asking them to forward relevant items to DHS?

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

Comments: Since the standard has been expanded to include “Attempts” the costs will increase incrementally regardless of the flexibility provided.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Seattle City Light appreciates the efforts of the SDT to provide flexibility in draft CIP-008-6. City Light also appreciates the work of the SDT to respond to industry comments from the first posting, and to provide extensive guidance documentation about the intent of the draft CIP-008 revisions and how the revised requirements might be implemented. For the most part, the revisions provide flexibility to meet reliability objectives in a cost effective manner, and the additional documentation offers reasonable assurance about acceptable means to meet these objectives.

In one area the modifications fall short, that of still requiring double-reporting of Reportable Cyber Security Incidents and attempted incidents to E-ISAC and to DHS NCCIC. This duplication of effort is neither cost effective for an entity nor is it the best use of scare resources during an actual cyber security incident to focus attention on a duplicative task. City Light urges the SDT to coordinate directly with NERC to arrange for E-ISAC to make the reportings to DHS NCCIC. Coordination of reporting is appropriate for E-ISAC both as part of its expanded industry engagement (and expanded budget) and in its central role as an analysis and sharing center, one step removed from the front lines of cyber issues at an entity. City Light understands that such a change might require additional negotiation among FERC, NERC, and E-ISAC, outside of the Standards process, but believes the result to be beneficial, appropriate, and consistent with the intent of FERC Order No. 848.

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	No
Document Name	
Comment	
We are concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have considerable costs and effort to accomplish these changes.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No
Document Name	
Comment	
Dependent upon what constitutes an “attempt”, additional resources (personnel and/or tools) may be needed to investigate and report on attempted events.	

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
We are concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have considerable costs and effort to accomplish these changes.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	

Tacoma Power is concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have to expend significant resources to comply with these changes. There is no evidence that reliability and security benefits will be commensurate with the increased costs.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

See our comments in the next question.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

The directives can be implemented with fewer changes to the Glossary terms and Requirements. Both should be changed as little as necessary to accomplish the directive and require the least revisions to Responsible Entity's existing programs. Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain and produce evidence for compliance monitoring without adding value to security or reliability.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Absent assurances from the appropriate authorities at the E-ISAC and the DHS that Responsible Entities will be able to use one reporting mechanism and one standardized report template for incident reporting, N&ST is concerned that the administrative overhead associated with filing and updating reports could be significant.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
NV Energy cannot make a determination on the implementation for this Standard being done in a cost effective manner given the current draft. Previous comments provided by NV Energy would require changes to the Definitions and Requirement that would support a more cost effective implementation.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
We do not agree. The directives can be implemented with fewer changes to the Glossary terms and Requirements. Both should be changed as little as necessary to accomplish the directive and require the least revisions to Responsible Entity's existing programs. **Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain and produce evidence for compliance monitoring without adding value to security or reliability, thus is no longer 'cost effective'**.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	No
Document Name	

Comment
With regard to reporting to two independent agencies (E-ISAC and NCCIC), it seems strange to have duplicate reporting. Would it not make sense to avoid such inefficiency by simply reporting to E-ISAC and asking them to forward relevant items to DHS?

Likes 0	
Dislikes 0	

Response

10, Provide any additional comments for the SDT to consider, if desired.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

The diagram in the Implementation guidance (page 6) references capitalized terms for "Attempted", "Compromise" and "Disrupt" which could be confusing to Responsible Entities.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

Regarding the Technical Rationale and Justification for Reliability Standard CIP-008-6, ERCOT requests that the historical rationale not be removed from the standard until this document is approved. If the content is removed and the Technical Rationale and Justification for Reliability Standard CIP-008-6 is not approved, valuable historical context for the full standard will disappear.

Regarding the implementation guidance, ERCOT requests that the historical Guidelines and Technical Basis not be removed from the standard until this document is endorsed by the ERO. If the content is removed and the Implementation Guidance for Reliability Standard CIP-008-6 is not endorsed, valuable historical context for the full standard will disappear.

ERCOT also offers the following comments on the Implementation Guidance:

- Page 7, typo correction: “Once this initial notification is made, if all attributes were known, they should have been included in the initial notification and the reporting obligation ends.
- Page 7 concern: It is noted that an entities reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC. This appears to indicate that entities are non-compliant up to this point. Requirement R4 allows partial reporting while maintaining compliance.
- Page 11 correction: The NERC Functional Model is not contained within Attachment 1 of CIP-002. The NERC Functional Model is a wholly separate document.
- Page 18 type: “Registered Entities are encouraged to explore options and tools designed to that take the guess work out of the process without being so overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs.”
- Page 18 concern: As noted in response to question 2, ERCOT has concerns with it being up to the Registered Entity to determine what constitutes and ‘attempt to compromise’. ERCOT recommends the SDT use industry-standard guidance to develop a baseline or minimum criteria for the industry.
- Pages 23-35 concern: ERCOT requests that the SDT consider removing the requirement language. This will ensure that the guidance is relevant and applicable beyond the current proposed version of the requirement language.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	
Document Name	

Comment

With regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three agencies during initial and updated submissions. If automation is not possible, consider adding a check box on the form indicating that E-ISAC needs to forward the report to NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency’s form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE’s responsibility to report

to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."
  In addition in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government*."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy appreciates the work the CIP-008-6 Standard Drafting team has done in the limited timeframe it was required to operate within. The second draft effectively addressed industry concerns from the first draft while preserving the intent of the Commission's directive. While Xcel Energy is voting Affirmative, there are a few language changes, in addition to the comments above, that would provide additional clarity. Those changes are as follows:

- In Requirements R2.1 the (S) was removed. We believe that this creates a subject-verb agreement issue. If we one were to say "*Test each Cyber Security Incident response plan at least once every 15 calendar months*:" than there is an indication that a Responsible Entity (RE) has more than one plan, many REs will only have one. However, if we were to say "*Test Cyber Security Incident response plan(s) at least once every 15 calendar months*:" it suggests that an RE may have one or more plans.
- The indication that REs need to have more than one plan is initially described in the already enforced parent Requirement of R2 where it states: "*Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include…*" If R2 were to read "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include…" and then state in "*Test Cyber Security Incident response plan(s) at least once every 15 calendar months*:" we would have agreement in the parent requirement an in the sub requirement that a RE can have one or more plans to collectively address each applicable Requirement.
- In R2.2 language is added that states: "…*that attempted to compromise a system identified in the "Applicable Systems" column for the Part*,…". It is not clear to which Requirement Part the *"Applicable Systems" column for the Part"* is referring to. Xcel Energy recommends adding the part number (i.e. Part 2.2) to each occasion where a Requirement Part is referenced with the Requirement Language or removing the references to the Part altogether.
- Generally, Xcel Energy SMEs feel that the changes made to CIP-008-5 in both Drafts 1 and Drafts 2 were done hastily and in a piecemeal way that were hard to follow and interpret. While Xcel Energy understands that this is likely a bi-product of the shortened drafting period created by the Commission, we also believe that NERC Standards need to be written in a concise and direct way so that no ambiguities exist nor interpretations needs to be made by Responsible Entities. When an existing Standard is open for modification or a new Standard is being

drafted, it is imperative that industry drafts a well written Standard that accomplishes the intent of mitigating the risk and eliminates all possible ambiguities that could lead to misinterpretations and possible compliance violations.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee

Answer	
Document Name	

Comment

In requirement R2, part 2.2, please consider changing the following text:

“Cyber Security Incident that *attempted* to compromise a system identified in the “Applicable Systems” column for the Part”

To: “Cyber Security Incident that *was only an attempt* to compromise a system identified in the “Applicable Systems” column for the Part “

In requirement R2, part 2.3, please consider changing the following text:

“Cyber Security Incidents that *attempted* to compromise a system identified in the “Applicable Systems” column for this Part. “

To: “Cyber Security Incidents that *were only an attempt* to compromise a system identified in the “Applicable Systems” column for this Part. “

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

: We support the extraordinary effort by the SDT, particularly with the extraordinarily short deadline from FERC. In FERC Order 848, ¶ 67, FERC stated, “the development of a Reliability Standard provides the Commission with an opportunity to review and ultimately approve a new or modified Reliability Standard, ensuring that the desired goals of the directive are met.” Moreover, the Reliability Standards development process allows for the collaboration of industry experts in developing a draft standard and also gives interested entities broader opportunity to participate and comment on any proposal that is developed.

The FERC directed timeframe and NERC's scheduling are NOT achieving FERC's statement that the development process allows collaboration and opportunity to participate and comment. The rushed timeframes, **especially a 15-day comment period that includes a holiday week is not acceptable**. Entities did not have time to engage experts within there organizations or trade associations. This comment period also overlaps with the comment period for multiple proposed massive changes to multiple CIP standards and definitions to address virtualization and other.

Won't agree to **define** "attempts" parameters.

There are no questions in the comment form for Part 2.2 or 2.3. We do not support the proposed changes to the Requirements language. *See comments in question #2*.

There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, **R4 only needs to refer to Reportable Cyber Security Incidents**. It does not need to include "a Cyber Security Indicent that was only an attempt to compromise a system identified in the "Applicable Systems" column. This phrase should be deleted.

Part 4.1: Include the following attributes, at a minimum, to the extent known: (4.1.1.-4.1.3 as proposed)

Part 4.2: Provide initial notification within the following timelines after determination of a Reportable Cyber Security Incident per Part 1.2: One hour after determination for compromises or disruptions. By the end of the next calendar day after determination for attempts.

Part 4.3: ok as proposed.

There are no questions in the comment form for the proposed Implementation Guidance or Technical Rationale and there has been insufficient time to review the amount of material presented in those two documents to provide comment with this draft. However, there are two initial comments.

Per the FERC Order 848, footnote 19 on page 13, the reference to reliability tasks says, the reliability tasks are referenced in the NERC Functional Model, not the BROS for CIP-002 as noted in the Implementation Guidance.

The Technical Rationale still refers to Reportable Attempted Cyber Security Incidents, *which is no longer a proposed defined term*, on page 4 in the first paragraph under Notification Timing.

All three Parts should follow the pattern in action-oriented Parts and start with verbs.

Dual reporting still not a resolved matter: It is not a consistent, and annonimity is not inplace for both required reporting entities. This needs to be addressed before going forward with this dual reporting requirement.

Refer to :

BROS for CIP-002

FERC Order 848, footnote 19 on page 13

FERC Order 848, ¶ 67

Freedom of Onformation Act

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417

*NCCIC – three things: Functional Impact, Level of Intrusion, Attack Vector…Compared to the NERC implementation guiadance – there is no contunity!

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

NV Energy would once again like to commend the SDT on the work done for this Standard, given the time constraints required for completing this project.

NV Energy would like to identify the following gaps between the comment questions and the CIP-008-6 Draft 2:

- There are no questions associated with this Draft's revisions to Requirement R2, Parts 2.2 and 2.3
- There are no questions associated with this Draft's revisions to Requirement R4
- There are no questions associated with this Draft's supplementary documentation: Implementation Guidance and Technical Rationale.

NV Energy believes there should be avenue for providing comments for all revisions within the Requirement language, and supplementary documentation.

NV Energy would also like to provide commentary on the poorly chosen timeframe for this commenting and balloting period for CIP-008-6. With the pool and commenting period opening on the Friday prior to the week of a federal two-day holiday, made it very difficult to engage our company experts, and trade associations, to review the revisions within this Draft. In addition to the holiday, the commenting and ballot period for CIP-008-6 is occurring concurrent to the commenting for the revisions to the CIP Standards due to Virtualization inclusion, which included extensive changes to CIP Glossary Terms and five (5) CIP Standards.

NV Energy understands that there is a strict timeline imposed for the approval of CIP-008-6, but this timeline should not impose on the industry's ability to provide fully vetted commentary and ballot position.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI believes that the SDT and NERC deserve recognition for exceptional work addressing FERC directives under a very aggressive timeline while still effectively considering and addressing Industry concerns.

One additional suggested minor change would be the following to Part 2.2:

"Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, ***and/or*** Cyber Security Incident that attempted to compromise a system ***as*** identified in the "Applicable Systems" columns ***under Requirement R1***, 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."

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	
Document Name	

Comment

Exelon would encourage the Standards Drafting Team (SDT) to assist Responsible Entities by providing a clear description in the Implementation Guidance of the scope of equipment in scope. Additional discussion around how PCA's are not included, as an example, will help entities properly scope their reporting program to the standard. We also believe it would be a good clarifying change to the definition of Reportable Cyber Security Incident to explicitly note that PCAs are not included in scope. We do not believe this is a substantive change to the standard, but reflects what is currently drafted. Additional explanation would be beneficial in clearly articulating scope of the standard.

Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
Although FERC requested reports be sent to both E-ISAC and NCCIC, this inefficiency may distract or impair a responsible entity's incident response. These government organizations should share reports instead of placing the burden on each entity.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
The addition of EACMS functions creates a second definition of the term. If the five functions are what the SDT considers an EACMS to fulfill, the official definition should be modified to include these to avoid differing interpretations of the term based on the Standard.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	

Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	

Comment
As per our response to Question 1, N&ST believes Protected Cyber Assets (PCAs) should be included with BES Cyber Systems and associated EACMS as applicable systems.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	
Document Name	

Comment
There are no questions in the comment form for Part 2.2 or 2.3. We do not support the proposed changes to the Requirements language. See comments in question 2. There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, R4 only needs to refer to Reportable Cyber Security Incidents. It does not need to include “a Cyber Security Incident that was only an attempt to compromise a system identified in the “Applicable Systems” column.” This phrase could be deleted. All three Parts should follow the pattern in action-oriented Parts and start with verbs. Part 4.1: Include the following attributes, at a minimum, to the extent known: (4.1.1.-4.1.3 as proposed) Part 4.2: Provide initial notification within the following timelines after determination of a Reportable Cyber Security Incident per Part 1.2: One hour after determination for compromises or disruptions. By the end of the next calendar day after determination for attempts.

Part 4.3: ok as proposed.

There are no questions in the comment form for the proposed Implementation Guidance or Technical Rationale and there has been insufficient time to review the amount of material presented in those two documents to provide comment with this draft. However, there are two initial comments.

The Implementation Guidance on page 11 below Figure 5 still references the BES Reliability Operating Services (BROS) with respect to reliability tasks. In the FERC order, the reference to reliability tasks is in footnote 19 on page 13. The footnote says the reliability tasks are referenced in the NERC Functional Model, not the BROS. See also the Commission Determination in FERC Order 791 paragraph 156, "While some commenters suggest that the phrase "reliability tasks" is best understood as referring to the bulk electric system reliability operating services listed in the Guidelines and Technical Basis section of CIP-002-5, we believe that the NERC Functional Model is the basis for the phrase "reliability task" while the Guidelines and Technical Basis section provides clarity on how the term applies to the CIP version 5 Standards."

The Technical Rationale on page 4 in the first paragraph under Notification Timing still refers to Reportable Attempted Cyber Security Incidents, which is no longer a proposed defined term. The capitalization should be removed.

We support the extraordinary effort by the SDT, particularly with the extraordinarily short deadline from FERC. In the Order, FERC stated in paragraph 67: "the development of a Reliability Standard provides the Commission with an opportunity to review and ultimately approve a new or modified Reliability Standard, ensuring that the desired goals of the directive are met. Moreover, the Reliability Standards development process allows for the collaboration of industry experts in developing a draft standard and also gives interested entities broader opportunity to participate and comment on any proposal that is developed.

The FERC directed timeframe and NERC's scheduling are NOT achieving FERC's statement that the development process allows collaboration and opportunity to participate and comment. The rushed timeframes, especially a 15-day comment period that includes a holiday week is not acceptable. Entities did not have time to engage experts within their organizations or trade associations. This comment period also overlaps with the comment period for proposed massive changes to multiple CIP standards and definitions to address virtualization and other.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	
Document Name	

Comment

LES supports the idea of timely information sharing with E-ISAC and in turn E-ISAC providing pertinent information to the industry. While the concern at hand is that not enough information is being provided to E-ISAC, the opposite also appears to be true in that many no-impact and isolated matters are sent out to the industry through E-ISAC alerts. Theses matter of no-impact (and no potential impact) do not appear to serve the industry well and instead only lead to alert fatigue. The drafting team may have an opportunity with their work on this issue to emphasize to E-ISAC that there is an opportunity for improvement in their analysis and their ultimate dissemination of entity provided information. The overall goal of this standard, in coordination with the work of the E-ISAC, should be to ensure the timely and full submission of pertinent data to E-ISAC and then providing the needed information to the industry through E-ISAC alerts.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	
Document Name	

Comment

We generally agree with the approach the SDT has taken. However, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	
Document Name	
Comment	

We agree with the comments provided by the IRC Standards Review Committee. While we are voting for the standard, we believe the following changes would improve and simplify the standard, while making it more adaptable to changing conditions:

- Regarding R2, we believe an implementation of the plan, to include notification of an incident or an attempt, should constitute a test of the plan. The measure for R2 should state this.
- R3 is redundant. The entity is responsible for having a plan in R1. They either have an appropriate plan or they don't. R3 adds an unnecessary obligation to have documentation to prove you have documentation.
- It is our understanding that some entities want additional structure on what gets reported. We believe a requirement on notification is sufficient and believe it should be up to the E-ISAC to work with the industry over time to define the information it needs when an incident gets reported. The structure of the report should not be hard-coded in the standard or an attachment.

Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	
Document Name	
Comment	

Comments: Duplicate effort would be needed to notify multiple agencies.

Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	
Document Name	
Comment	

Referring to the "Applicable Systems" column in the "Requirements" column may be redundant. A suggestion for the language in the Part 2.2 is: "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 was an attempt to compromise (as defined in Part 1.2.1) one or more applicable systems, 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”

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	
Document Name	

Comment

We do not find language reflecting provisions for CIP Exceptional Circumstances within CIP-008, so there is no safe haven in the event of “*A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure****; a Cyber Security Incident requiring emergency assistance****; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.” It seems that CIP-008 should have language related to CEC as well.*

We understand from the CIP-008 revisions webinar that the SDT declined to include this as part of this project. We strongly encourage the SDT to incorporate language to support CEC relative to CIP-008 as this standard will likely be filed with FERC prior to the completion of the Ballot Process for CEC under Project 2016-02.

Likes 0	
Dislikes 0	

Response

William Sanders - Lower Colorado River Authority - 1

Answer	
Document Name	

Comment

As responsible entities will be required to report more detailed cybersecurity incident information with both E ISAC and DHS once CIP-008-6 becomes effective, both organizations (E ISAC and DHS) should provide a secure electronic method for reporting incidents using existing portals or other means.

Likes 0	
Dislikes 0	

Response
Teresa Cantwell - Lower Colorado River Authority - 5
Answer	
Document Name	
Comment
As responsible entities will be required to report more detailed cybersecurity incident information with both E ISAC and DHS once CIP-008-6 becomes effective, both organizations (E ISAC and DHS) should provide a secure electronic method for reporting incidents using existing portals or other means.
Likes 0	
Dislikes 0	
Response
Barry Lawson - National Rural Electric Cooperative Association - 4
Answer	
Document Name	
Comment
NRECA appreciates the efforts of the SDT on this project and also thanks the SDT for the modifcations made in response to our comments.
Likes 0	
Dislikes 0	
Response
Andrea Barclay - Georgia System Operations Corporation - 4
Answer	
Document Name	
Comment
We appreciate the efforts of the SDT on this project and also thanks the SDT for the modifcations made in response to our comments.
Likes 0	
Dislikes 0	
Response

Patricia Boody - Lakeland Electric - 3	
Answer	
Document Name	
Comment	

We do not find language reflecting provisions for CIP Exceptional Circumstances within CIP-008, so there is no safe haven in the event of "*A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure****; a Cyber Security Incident requiring emergency assistance****; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability." It seems that CIP-008 should have language related to CEC as well.*

We understand from the CIIP-008 revisions webinar that the SDT declined to include this as part of this project. We strongly encourage the SDT to incorporate language to support CEC relative to CIP-008 as this standard will likely be filed with FERC prior to the completion of the Ballot Process for CEC under Project 2016-02.

Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	
Document Name	
Comment	

Change the sentence in CIP 008 R2 Part 2.2: The sentence currently reads "Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Reportable Attempted Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, or performing an exercise of a Reportable Cyber Security Incident." Change to "Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, or performing an exercise of a Reportable Cyber Security Incident."

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Recommend the SDT consider including "Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column" to Part 2.1 in one of the scenarios for testing each Cyber Security Incident response plan. A test of the plan should address all required Parts from R1 no matter the scenario, whether Reportable or attempted Cyber Security Incidents, and exercise SMEs ability to discern the difference.

Recommend the SDT consider adding Physical Security Perimeter (PSP) or associated Physical Access Control Systems (PACS) into the applicable systems for CIP-008-6 to ensure any attempts, successful or unsuccessful to compromise the responsible entities PSP or associated PACS are obtained to gain a better understanding of the full scope of cyber-related threats facing the Bulk-Electric Power System(s).

Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	

Seattle City Light supports these changes in principle, but casts a NO ballot for two reasons. One, to encourage another effort at creating a single report (see discussion in Question 9, above). And two, to encourage additional implementation guidance to add clarity as to how each action reflects a reliability objective and to discuss alternatives to the single approaches, in most case, that are presented.

City Light has two additional questions about proposed CIP-008-6. One, there is a necessity to notify the local Reliability Coordinator if a BROS capability has been compromised. Clarification would be helpful of how this process is envisioned to work in conjunction with CIP-008-6 notificaitons and EOP-004 notifications. Two, what is done with notification information entities make to E-ISAC and DHS? Additional documentation is desired about the subsequent sharing, processing, and storage of notification data, so that appropriate Federal designations (CEII or similar) may be made as appropriate.

Finally, Seattle City Light also would like to propose that the SDT consider the possibility that, if an entity participates in the voluntary E-ISAC CRISP program, such participation would automatically satisfy all reporting requirements of CIP-008. CRISP is a public-private cyber threat and data sharing platform coordinated by E-ISAC and DOE. Participants voluntarily share IT system traffic in near-real time by installing an information-sharing device at the border of the IT systems, just outside the firewall.

Such an approach to CIP-008 reporting has a double benefit. It encourages greater participation in CRISP, which in turn increases the value of the program. It also provides an increased flow of raw cyber security data from industry. This would be an opportunity for FERC and NERC to offer entities a carrot in place of the usual reliability Standard stick.

Other similar IT data sharing platforms, such as that being developed by DHS, might be afforded similar standing as regards CIP-008 reporting.

Additional information about CRISP is available here: https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
See MRO's NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF recommends that the SDT add language around the Requirement to report “attempt to compromise” recognizing Entities are allowed flexibility by detrmining their criteria based on each entity’s architecture and that a “singular criteria” (one size fit all) will not be effective for applicable entities. We further recommend that this guidance be within the Implementation Plan or Guidance documents that the SDT has developed.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

CIP-008-5 applicability addresses high and medium impact BCS and their associated EACMS, however, it is also recommended to address PCAs as part of the scope. As the new draft definition of a Cyber Security Incident and Reportable Cyber Security Incident reference "the attempted compromised or the compromise of an Electronic Security Perimeter", how can PCAs not be included or are they implied? In the CIP-005-5 Table R1 – Electronic Security Perimeter the Applicable Systems column within the CIP-005-5 Standard PCAs associated with High and Medium Impact BES Cyber Systems are included and make up an Electronic Security Perimeter (ESP). Not listing or including PCAs in the applicability section of CIP-008-6 is inconsistent with the current CIP-007-6 and CIP-010-2 Standards as they ensure the same level of preventative security controls and baselines are applied to PCAs that make up the ESP as a whole.

Part 2.1 should be modified to permit exercise of the plan using any Cyber Security Incident. Restricting the exercise to only Reportable Cyber Security Incidents restricts the exercise to only a subset of an entity's incident response plan. Part 2.2 should be simplified to require use of the incident response plan when responding to any Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	
Document Name	

Comment

AZPS respectfully recommends removal of the word "only" from the following:

- Part 1.2.2
- Measures for Part 2.3
- R4

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

In requirement R2, part 2.2, please consider changing the following text:

"Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part"

To

“Cyber Security Incident that was only an attempt to compromise a system identified in the “Applicable Systems” column for the Part “

In requirement R2, part 2.3, please consider changing the following text:

“Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part. “

To

“Cyber Security Incidents that were only an attempt to compromise a system identified in the “Applicable Systems” column for this Part. “

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	
Document Name	

Comment

Reclamation recommends Requirement R1 Part 1.1 be changed

from:

One or more processes to identify, classify, and respond to Cyber Security Incidents.

to:

One or more processes to identify, classify, handle, and respond to Cyber Security Incidents.

After the change to Requirement R1 Part 1.1 is made, Reclamation recommends the SDT change the measure in Requirement R1 Part 1.1

from:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

to:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, handle, and respond to Cyber Security Incidents (e.g., containment, eradication, recovery/incident resolution).

After the change to Requirement R1 Part 1.1 measure is incorporated, Reclamation recommends the SDT remove Requirement R1 Part 1.4.

Reclamation also recommends changing the timeframe specified in Requirement R3 Part 3.2 to 90 days to align with the time allowed in Requirement R3 Part 3.1.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

AECI supports comments provided by NRECA

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	
Document Name	

Comment

We agree with the direction of the Drafting team, but are concerned that there is not enough protection from subjective enforcement by auditors and enforcement staff. The danger is most apparent when the entity is trying to meet the spirit of the standard but held to a best practices threshold.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
No comment from SRP	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	
Document Name	
Comment	
AEP recommends striking the word “only” from the sentences which include, “….Cyber Security Incident was only an attempt to compromise a system identified in the “Applicable Systems” column for this Part.” In requirement R4 and part 4.2. This is to be consistent with requirement parts 2.2 and 2.3 and the definition of Cyber Security Incidnet.	
Likes 0	
Dislikes 0	
Response	

Comments received from Jack Cashin, APPA

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

Yes
x No

Comments:
APPA believes that additional guidance on the language on alternative approaches -- “establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable system,” is needed.
Public power concurs that PCAs should not be included in the proposed modification to the standard.

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

X Yes
No

Comments: APPA supports the intent of the proposed changes but, as stated in the answer to question 1, believe the Standard would benefit from guidance on alternative approaches addressing the language,“establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.”
We are concerned that without established guidance, complying entities and compliance and enforcement staff do not have sufficient guidance to come to a common understanding of the draft standard language. Complying public power entities believe that a conservative reporting criteria will present significant costs to administer without corresponding measurable reliability benefits. The costs required for the follow-up requirements in R4 are significant.

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

X Yes
No

Comments: APPA believes that the proposed changes reflect that an Entity must have a process in place to identify compromise attempts and provide notification. Public power is concerned that specifying a specific number of days for reporting actual, and attempted Cyber Security Incidents to agencies could lead to resource challenges. Public power recommends that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1. Physically getting a team to remote substations to determine the attack vector could take time, and the difficulty will increase depending on how wide-spread the event turns out to be.

4. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? Please provide comments and an alternate approach to addressing the directive, if possible.

x Yes
No

Comments: Because there is another SDT evaluating the term EACMS, APPA would appreciate further guidance from the CIP-008 SDT on whether just the proposed EACS or both the proposed EACS and EAMS would be included in the revised CIP-008 requirements.

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

Yes
X No

Comments: APPA appreciates that the SDT has provided additional time for updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement of tracking the periodic updates will add additional administrative burden for utilities and may not add commensurate reliability benefits.

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

Yes
No

Comments: It is not clear what the SDT means with the language, "flexibility to determine notification methods in their process." Is this referring to language in the R 4.2 that was deleted in this version? Otherwise, the "flexibility" is not included. The measures for the new R 4.2 state just a single measure: Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

X Yes
No

Comments: APPA supports the extended implementation timeframe.

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

Yes
No

Comments:

9. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Yes
X No

Comments: Public power is concerned that the timeline for reporting creates additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have to expend significant resources to comply with these changes. There is no evidence that reliability and security benefits will be commensurate with the increased costs.

10. Provide any additional comments for the SDT to consider, if desired.

Comments received from Brenda Hampton, Luminant Mining Company LLC

Question 1
Luminant agrees with the updated approach; however, the language in 1.2.2 might be improved. Luminant suggests simplifying by combining the bullets to read: "Determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise one or more systems identified in the “Applicable Systems” column for this Part; and"

Question 6
Luminant agrees with providing flexibility to the entity; however, we continue to disagree with the determination that reporting to a single agency as an intermediary to the other agency is outside the scope of the SAR. We also suggest NERC pursue an update to OE-417 to add a checkbox to include the DHS organization (in this case NCCIC). We believe every effort should be made to consolidate reporting to a single entity.

Question 10
Although we believe that it is in industry's best interests to come up with criteria for evaluating "attempts to compromise", we are absolutely opposed to the Implementation Plan as it currently exists. The suggested criteria would leave entities with a ridiculously broad criteria for reporting. We suggest a robust process may be required to come up with better criteria for this category and may need some trial period before finalizing any IP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-6

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting: Consideration of Comments

January 2019

RELIABILITY | ACCOUNTABILITY



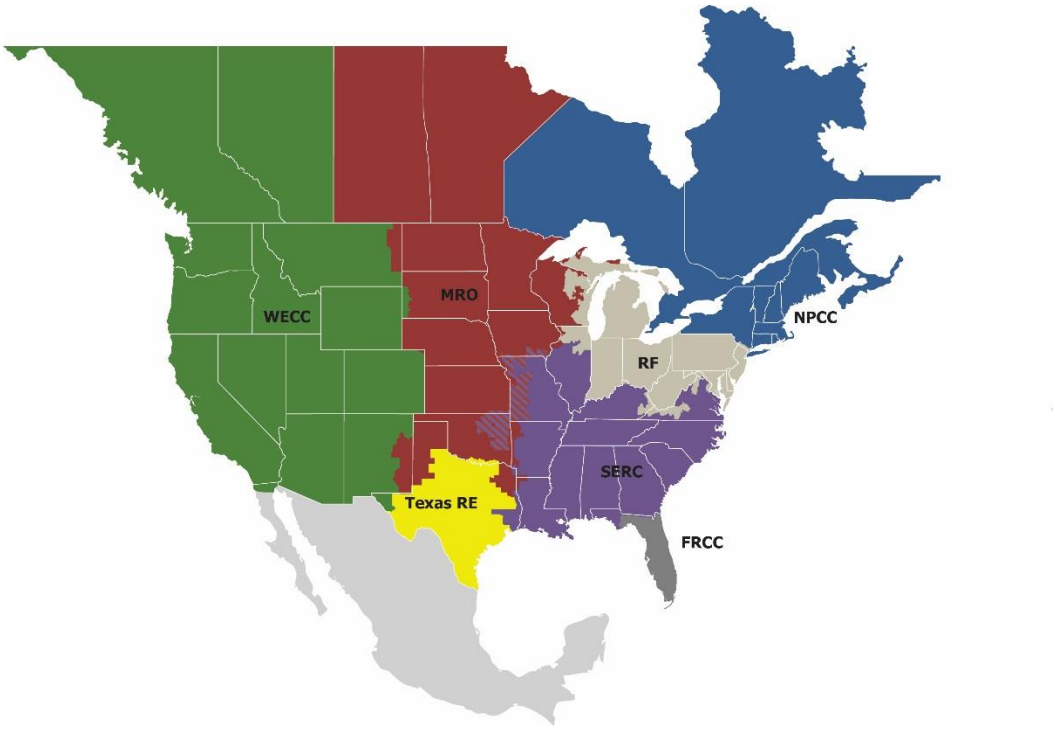

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven regional entities (REs), is a highly reliable and secure North American Bulk-Power System (BPS). Our mission is to ensure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries, as shown below in the map and corresponding table. The downward diagonal, multicolored area denotes overlap because some Load-Serving Entities participate in one region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team thanks all commenters who submitted comments on the draft CIP-008-6 standard. This standard was posted for a 10-day public comment period, ending Thursday, November 29, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 72 sets of responses, including comments from approximately 160 different people from approximately 110 companies, representing 7 of the Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Alison Oswald, at 404-446-9668 or at alison.oswald@nerc.net.

CIP-008-6 Consideration of Comments – Summary Responses

Purpose

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team (SDT) appreciates industry's comments on the CIP-008-6 standard. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and the SDT's corresponding responses. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Definitions

Several commenters requested the SDT modify the Cyber Security Incident definition to clarify it to include both disruption and compromise for all sub points the way the RCSI definition does.

The Cyber Security Incident definition includes: "compromises, or was an attempt to compromise" in its first bullet, and "disrupts, or was an attempt to disrupt," in its second bullet. The SDT asserts that both terms are addressed within the definition. The SDT was purposeful when associating compromise with the cyber systems and perimeters whereas disruptions are related to the function or reliability task. This distinction helps further clarify what is in scope for low impact BES Cyber Systems.

One commenter suggested adding PSP to RCSI definition.

Regarding PSPs, the currently enforceable definition of Cyber Security Incident includes malicious acts or suspicious events that compromise, or attempt to compromise, PSPs. The currently-enforceable Reportable Cyber Security Incident definition includes Cyber Security Incidents that have compromised or disrupted one or more reliability tasks of a functional entity. As such, compromises or attempts to compromise PSPs could be reportable under the currently enforceable standard and definition. Cyber Security Incident that compromises or attempts to compromise a PSP would become reportable under the RCSI definition when it results in a compromise or disruption of one or more reliability tasks.

Commenters requested the SDT modify the Reportable Cyber Security Incident definition to delete "that performs one or more reliability tasks of a functional entity."

Thank you for your comment, the team asserts that the inclusion of the phrase "that performs one or more reliability tasks of a functional entity" in the Reportable Cyber Security Incident definition adds additional clarity and has elected to leave it in the proposed definition. In addition, it is consistent with previous versions of CIP-008.

Several commenters expressed concern that low impact could be interpreted as in scope as a function of the Cyber Security Incident definition.

The SDT addressed this concern by moving "high and medium impact" in front of BES Cyber Systems and ESP, PSP and EACMS in the first bullet of the Cyber Security Incident definition. The SDT asserts this single change also addresses the concern for the Reportable Cyber Security Incident definition.

Some commenters requested that the SDT modify the RCSI definition to include reportable attempts.

The SDT understands there could be some confusion, but the team strived to strike a balance between clear reporting definitions and timeframes commensurate with risk related to reporting attempts and RCSI. The SDT asserts that a change to the RCSI definition could affect more than CIP-008 and have consequences relative to CIP-003.

One commenter asserted that the definition of the revised terms was not provided.

The SDT thanks you for your comment. The revised terms were provided in the New or Modified Term(s) Used in NERC Reliability Standards section of the draft standard.

Reporting

While the majority of the commenters appreciated the extended notification timeframes provided in Requirement 4, Parts 4.2 and 4.3, several commenters again requested the inclusion of CIP Exceptional Circumstances (CEC).
The SDT foremost asserts that a general review of CEC is ongoing as part of the scope of Project 2016-02. The SDT further asserts that waiving the notification requirements when faced with a situation that involves or threatens to involve an imminent or existing hardware, software, or equipment failure, or a Cyber Security Incident requiring emergency assistance, is in direct contradiction to the intent of FERC Order No. 848. It is in exactly these types of situations where it is most important to share information amongst sector entities to stave off similar threats to protect the reliability of the BES.

Several commenters stated that the notification timeframes were confusing, inappropriate for updated information, or unduly burdensome. Also, a concern was raised that specifying a specific number of days for reporting actual and attempted Cyber Security Incidents to agencies will sometimes be a resource challenge. The recommendation is that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1.
The SDT asserts that it is within each entity's purview to define its own criteria for and determination of reportability and knowledge of attributes. Throughout the requirement compliance timing begins with each determination as the entity executes its response process. It is upon the entity's determination that the notification timeframes are predicated — whether it is one hour from determination that an attempt to compromise is now a Reportable Cyber Security Incident, or whether it is within seven days after the determination of new attribute information. It is not the SDTs intent for an entity to rush their incident response process. Initial notifications can be preliminary and include only information that is known at the time of determination. Additional attribute information that is determined as the investigation continues should be reported per the update timeframes in the standard.

A commenter requested that the notification timeframes be consistent for Parts 4.2 and 4.3, specifically seven days after determination for an initial notification, as well as updates.
The SDT asserts that seven days after determination for an initial notification is not an appropriate reporting threshold. The reporting timeline for attempts to compromise is in alignment with FERC Order No. 848, p 89 and is in the spirit of timely reporting for information sharing. In addition, the one-hour initial notification timeframe for Reportable Cyber Security Incidents is not new and entities should already have processes in place to satisfy that requirement.

A commenter expressed concern about reporting to two different agencies and requested doubling the timeframe for initial notification to accommodate the additional agency reporting requirement.
FERC Order No. 848 instructs the SDT to consider risk when developing timeframes. The SDT asserts that the 1 hour timeline is in alignment with previous versions of CIP-008, other FERC orders, and severity of the incident. This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable. It does require preliminary notification, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report. The SDT also asserts that means exist to provide simultaneous notification. The time required to notify additional entities does not begin until the entity has made a determination that aligns with a reportable classification.

Several commenters requested coordination amongst the electric sector's event notification requirements, i.e., U.S. Department of Energy (OE-417), EOP-004, and CIP-008. Also, some commenters would like to leverage reporting to E-ISAC as an intermediary to NCCIC.
The SDT determined not to modify existing reporting forms, such as OE-417, because Order No. 848 noted that this form did not request information that FERC directed the SDT to require in CIP-008. Nonetheless the SDT notes that entities may consider synchronizing their reporting processes as long as all information that is required to be reported is submitted to appropriate agencies.

The SDT asserts that the proposed reliability standard is responsive to FERC Order 848 and that E-ISAC acting as an intermediary is outside of the scope of the SAR.

Some commenters would like to leverage reporting to a single agency as an intermediary to the other agency.
The SDT thanks you for your comment, however the SDT asserts that the proposed reliability standard is responsive to FERC Order 848 and that this is outside of the scope of the SAR.

Many of the commenters, expressed the desire to have a Standardized Reporting form and to submit one report for automatic submission to the two entities.
While the initial form that was developed is not required, it is included as an example in Implementation Guidance and available for use. The SDT has preserved the entity's ability to choose to use that form or not.

One commenter expressed concern that auditor will use subjective judgement.
Thank you for your comment. The SDT wanted to give flexibility to entities in creating their process to accommodate differing size entities while meeting the requirements in the FERC order. The SDT has been working in close collaboration with the RSAW Task Force developing the CIP-008-6 RSAW.

One commenter stated that Part 4.2 stands on its own and notification is part of "respond" in Part 1.1 and does not need Part 1.2. Part 4.2 should be clarified so show that all events that meet the definition of "Cyber Security Incident" are reportable, but that only actual compromise or disruption is reportable within one hour.
This concern has been addressed by adding clarifying language to each of the applicable parts. It is not the intent of the SDT to infer that all Cyber Security Incidents are reportable. Rather, the SDT has developed standards requirement language that provides entities with the flexibility to create processes and criteria to ascertain what is reportable.

EACMS and Scoping

Two commenters asked that the SDT limit EACMS in the applicable systems column to exclude systems solely performing monitoring functions.
The SDT reevaluated FERC Order No. 848 and asserts that two of the five functions listed within the directive in Paragraph 54 (monitoring and logging, and alerting) are intentionally included.

One commenter stated that the addition of EACMS functions creates a second definition of the term. If the five functions are what the SDT considers an EACMS to fulfill, the official definition should be modified to include these to avoid differing interpretations of the term based on the Standard.
The SDT removed the mention of the five functions within the standard and the current definition of EACMS stands. NERC Project 2016-02 is also in the process of modifications to the NERC Glossary of Terms definitions for Interactive Remote Access, Intermediate Systems, and Electronic Access Control or Monitoring Systems. Additionally, the Project 2018-02 SDT has decided not to modify these terms due to their pervasive use throughout CIP Reliability Standards and the abbreviated timeline for filing of CIP-008-6 as directed in FERC Order No. 848.

One commenter disagrees with the inclusion of EACMS.
Thank you for your comment, the SDT asserts that EACMS is include per FERC order 848 Paragraph 54.

One commenter requested the SDT add ESPs to Applicable Systems in R1.2.2 and R4.2.
The SDT thanks you for your comment. The applicable systems in the proposed standard meet FERC Order 848 for the systems to be included.

Some commenters expressed concern that attempts to compromise potentially expand the scope to assets that are corporate systems or otherwise not associated with the CIP program.

The SDT added clarifying language to both the definitions and requirements in an effort to ensure that the scope was limited to the appropriate Applicable Systems.

Requested Modifications to Standard Language

Several commenters requested that the SDT define attempts to compromise, define criteria for attempts to compromise; or define a minimum set of criteria for attempts to compromise.

The SDT thanks commenters for their input. The SDT asserts that it is to the industry's benefit that CIP-008 leaves it up to each Responsible Entity to document a process to determine what constitutes an "attempt to compromise", as well as defining criteria for "attempts to compromise;" or defining a minimum set of criteria for "attempts to compromise."

The SDT further asserts that no two Responsible Entities are alike and the determination of "attempts" and criteria for "attempts" is contextual and dependent on what is normal within each unique organization.

To define "attempt" or criteria for "attempts" could create an overly prescriptive and less risk-based approach and may have the unintended consequence of undue administrative burden or removal of needed discretion and professional judgment from subject matter experts.

In order to futureproof the standard the SDT determined that it was not to the benefit of Responsible Entities to define any fixed sets of criteria for "attempts to compromise" based on :

- The current state of cyber security threats will continue to evolve and that the associated security technologies will also evolve in response to these threats. The criteria for "attempts to compromise" will also evolve over time as a result

- Embedding criteria based on current technical requirements (such as those from CIP-007-6 R4.1) and/or direct references to other CIP standards such as CIP-007-6 R4.1 creates an administrative issue when changes to those technical requirements or the referenced standards are required.

The SDT has developed proposed Implementation Guidance inclusive of several examples in an effort to address this.

The team received comments stating that they appreciate the flexibility to establish our own criteria, they believe that this flexibility will be addressed in a future NOPR as all applicable entities will have different criteria of what an attempt to compromise is.

The SDT thanks you for your comment. The SDT strived to strike a balance between flexibility and consistency in the standard. The SDT believes this meets FERC order 848 and provides flexibility in implementation and future proofs the standard. This approach reflects the approach taken in other current enforceable standards, whereby the entity defines the criteria that best meets their unique operating environment.

Some commenters stated that "attempts" have been a part of the definition for a Cyber Security Incident for more than a decade and the entity does not support a process to define "attempts."

The SDT sought to create language that allows the entity flexibility to work the definition for attempts into their processes in a manner that supports the FERC order 848 reporting requirement directives and accommodates unique operating environments.

Many commenters recommend striking the word "only" from the sentences which include, "….Cyber Security Incident was only an attempt to compromise a system identified in the "Applicable Systems" column for this Part."

The SDT thanks you for your comments. The word "only" has been removed from the final version of the standard.

One commenter stated that referring to the "Applicable Systems" column within the "Requirements" column was redundant and confusing.

The SDT asserts that this reference provides additional clarity for the narrowed scope of reportable attempts to compromise.

Some comments were received regards to the structure of Requirements R1.1 and R1.2. It was suggested that R1.1 include having a process and using it.
The SDT thanks commenters for their input. The SDT structured R1.1 as the requirement to a have one or more processes and R1.2 as the required elements for the contents of these process or processes. Requirement R2.2 requires the use of the processes defined in R1.

Some comments received that suggested R1.2 language was not worded correctly.
The SDT thanks commenters for their input. The intent was R1.2 contains elements of what is required in R1.1. The SDT has made clarifying changes to the standard to address this concern.

One commenter suggested the use of "method" instead of "criteria" in R1.2.1.
The SDT considered whether wording using "method" was a less prescriptive than using "criteria". At this time, the SDT feels that these words are effectively equivalent. The SDT did make other changes to clarify the wording in R1.2.1.

Some comments were received that double jeopardy exists between Requirement R1.2.3 and R4.
The SDT structured R1.2.3 as a required element of the process(es) needed for Requirement R1.1.
R4 is the requirement that defines to whom reports are required, the attributes to be reported and the timelines required. R1.2.3 and R4 are cascaded requirements and do not create a double jeopardy.

One commenter would like to see the reporting of an "attempt" to also constitute a test of entity incident response plan in R2.
Thank you for your comment, the SDT intentionally excluded attempts to compromise from Requirement R2, Part 2.1. Please see Technical Rationale for justification.

PCAs

Some commenters indicated that PCAs should be included as part of the applicable systems.
The SDT thanks commenters for their input. The SDT has determined that the addition of PCAs to the applicable systems may create additional administrative burden given that:

- PCAs were not specifically discussed within FERC order 848, appearing only in P10 in reference to EACMS and ESP
- PCAs do not perform BES Reliability Operating Services that fall within the 15 minute criteria defined in CIP-002 and have a much lower risk profile
- While logging requirements are similar to BCS/BCA, PCA user authorization is currently not part of the CIP-004 program. While many entities already have existing user authorization programs for PCAs, adapting these existing programs into their CIP user authorization program may require extensive rework

The SDT asserts that entities retain the ability to voluntary report on PCA's as deemed appropriate and have added information to the Implementation Guidance to address this.

VRF/VSLs

Some commenters noted that some of the VSLs seem to be duplicative in the Severe and High columns for Requirement R4.
While the language is similar in both the High and Severe columns, the Severe uses "and" whereas the High uses "or." The intent was that if an entity failed to notify both E-ISAC and NCCIC, it violated the standard to a greater degree than only failing to notify one agency ("or") of a Reportable Cyber Security Incident.

Some commenters recommended the SDT consider how an auditor would interpret the standard to determine VSLs.
The SDT does not consider audit approach in determining VSLs. VSLs are one factor in assessing penalties after it has been determined the entity has violated the requirement. At that point, enforcement staff has reviewed the audit team's recommendations and determined that there has been a violation. When developing VSLs, the SDT considers whether an entity may still be in compliance with some parts of the requirement while violating others and assigns the VSLs accordingly.

Some commenters suggested moving the process to define attempts to compromise to a lower VSL than the process to identify Reportable Cyber Security Incidents and suggested putting other parts of Requirement R1 in the Lower and Moderate columns.
The SDT considered separating the tiers but ultimately determined not to change the severity level for attempts within Requirement R1. The SDT determined that the failure to include a process to define attempts or a process to identify Reportable Cyber Security Incidents in the Cyber Security Incident response plan are a similar degree of violation of Requirement R1. The SDT also determined that the other parts addressing the processes required to be included belonged in the Moderate column. Finally, the SDT determined not to lower the VSLs of some of the currently enforceable requirements from CIP-008-5.

Some commenters asserted that the VSLs do not appropriately reflect risk to BES reliability.
VSLs reflect degrees of compliance with the requirement, not risk to the BES. VRFs are indicators of impact to the BES if a requirement is violated. As the VRFs for R1 and R4 are Lower, the SDT asserts that they accurately reflect the risk of these administrative requirements.

One commenter noted that failure to notify the applicable agencies of an attempted Cyber Security Incident should not result in a severe penalty.
VSLs are just one factor in the determination of a penalty amount, so putting a requirement in the "Severe" VSL category does not necessarily mean that a Responsible Entity will receive a severe penalty. However, the particular violation the commenter describes would fall under the "Moderate" VSL category.

Some commenters noted that the VSLs are administrative in nature, could cause unnecessary violations, or should not have a Severe VSL.
The SDT notes that VSLs are considered for penalty sanctions after a violation has been determined based on the language of the requirement. Pursuant to the VSL Guidelines based on the 2008 FERC "VSL Order," Violation Severity Levels must have a severe category as VSLs represent degrees of compliance, not risk to the BES. A severe VSL means that an entity did not meet the performance of the requirement, whereas lesser VSLs show that an entity met some performance of the requirement but not all of the requirement. The SDT agrees that Requirement R4 is administrative in nature so it assigned a "Lower" VRF to reflect the requirement's impact to reliability if violated. However, this consideration would not factor into how VSLs are determined.

Some commenters noted that they did not agree with the VSLs because of the requirement language or could not comment on the VSLs because of changes they recommended to the requirement language.
The SDT considered these comments when reviewing the requirement language.

One commenter noted that the shortened ballot period did not allow them to evaluate the VRFs or VSLs and another commenter noted disagreement with the VRFs and VSLs but did not think proposing alternatives would be considered.
The SDT understands this was a shortened comment period and ballot but appreciates industry's cooperation in meeting the 6-month deadline to file CIP-008-6 with FERC. Also, the SDT appreciates when commenters provide alternatives if in disagreement with the language.

Implementation Plan

A few comments were received that requested a 24 month implementation plan.

The SDT received comments regarding the timeframe for the Implementation Plan on the first ballot and the team adjusted from 12 to 18 months. The SDT assert that an 18-month implementation timeline is appropriate as it strikes a balance between the FERC directive for an expeditious implementation and capabilities of industry.

A few comments supported a 12 month implementation plan and one stated "This standard would need to be revised again if Project 2016-02 is implemented and the definition for EACMS changes. If the implementation timeline is extended too far, a conflict could add more work."

Based on the timing of Project 2016-02 and the current proposed changes, the SDT asserts that the net effect will not have significant impact on CIP-008-6.

One commenter asked what the SDT's intent for the initial performance of Part 2.1 and requested this be addressed in the Implementation Plan.

Thank you for your comment. The SDT chose not to include a section for the initial performance of certain period requirements in the interest of preventing confusion and in deference to the existing CAN-012 which clearly states, "[I]n the event that the standard or implementation plan is silent with regard to completing a periodic activity, CEAs are to verify that the registered entity has performed the periodic activity within the standard's timeframe after the enforceable date."

Cost Effectiveness

One commenter noted concern that the timelines for reporting may create additional administrative burden and cost.

The SDT understand there are cost considerations with every change to the standard. However, the SDT asserts, that the changes are not overly burdensome and balance added security, information sharing and the directives from the FERC order 848.

One commenter noted "the directives can be implemented with fewer changes to the Glossary terms and Requirements. Both should be changed as little as necessary to accomplish the directive and require the least revisions to Responsible Entity's existing programs."

The SDT asserts that we made the fewest changes possible to meet FERC order 848. For example, the SDT removed the original proposed definition of Reportable Attempted Cyber Security Incident. The SDT also asserts that we carefully considered the impact to other standards to minimize the impact.

One commenter noted that the standard falls short in the area requiring double-reporting of Reportable Cyber Security Incidents and attempted incidents to E-ISAC and to DHS NCCIC. This duplication of effort is neither cost effective for an entity nor is it the best use of scarce resources during an actual cyber security incident to focus attention on a duplicative task.

The SDT understands the concern about dual reporting but in order to meet the directives in FERC order 848, dual reporting is required. The SDT took efforts to ensure that entities could determine their methods of reporting in ways that minimize duplication of efforts such as co-copying on an email message**.** By giving the entity the ability to make their determination of when something is a Reportable Cyber Security Incident or an "attempt" the entity determines reporting clock start.

One commenter stated that the new standard ultimately requires Responsible Entities to become cyber security threat hunters rather than relying on the protections required within the CIP standards and requires investment in a 24x7x365 Security Operations Center (SOC). In addition, there is no reduction in risk to the BES in reporting attempts to compromise.

Thank you for your comment. The SDT asserts that the modifications do not require an entity to establish and implement a 24x7x365 Security Operations Center to achieve compliance, rather the entity may perform these activities on a schedule that is appropriate for their unique operating environment that is documented in their process. At a minimum, these modifications to this standard add formality around reporting for events that are detected and evaluated under existing enforceable standards with the intent to reduce risk to the BES through more timely information sharing and enhanced situational awareness that the expanded reporting will provide.

One commenter stated dependent upon what constitutes an "attempt", additional resources (personnel and/or tools) may be needed to investigate and report on attempted events.
The SDT asserts that the requirement has been written in a manner to provide the entity the flexibility to establish criteria and processes to determine what constitutes an attempt such that they may operate and achieve compliance in a cost effective way.

Some commenters noted that they could not comment on the cost effectiveness of the standard because of changes they recommended to the requirement language.
The SDT considered these comments when reviewing the requirement language.

One commenter expressed concerns with the scoping of the Standard Authorization Request process.
Thank you for your comment, the SDT asserts that the SAR, authorized by the Standards Committee was adequately scoped to meet the directives of FERC order 848. SAR development was prior to the establishment of the Standards Drafting Team (SDT).

Other

Some commenters expressed concern over the shortened timeframe of the project.
The SDT thanks you for your response. We understand that the accelerated timeline could have created a situation where comments were on a shorter timeframe. While there were some scheduling challenges the SDT did the best to balance the timeframe with industries availability. In addition, the standard drafting process requires NERC Board of Trustee approval before filing with FERC to meet order 848 deadline of April 1, 2019.

A comment was received that stated the comment form did not provide specific questions for every requirement and all supporting documentation.
Thank you for your comment. In an attempt to keep the comment form concise, the SDT offered questions on the comment form for the major changes from the previous draft of the standard. The SDT asserts that there is always an opportunity to respond to any area of the standard in the last "catch all" question.

On commenter stated that the overall goal of this standard, in coordination with the work of the E-ISAC, should be to ensure the timely and full submission of pertinent data to E-ISAC and then providing the needed information to the industry through E-ISAC alerts
The SDT thanks you for your comment. During this process the SDT worked closely with E-ISAC to discuss issues with them. While there are always issues with balancing information that is received, the E-ISAC provides opportunities to entities to adjust the way they are receiving information.

Regarding the Technical Rationale and Justification for Reliability Standard CIP-008-6, ERCOT requests that the historical rationale not be removed from the standard until this document is approved. If the content is removed and the Technical Rationale and Justification for Reliability Standard CIP-008-6 is not approved, valuable historical context for the full standard will disappear.
The SDT thanks you for your comment, the Guidelines and Technical Basis will be included in its entirety within the TR and the IG for historical reference. It should also be noted that previous versions of the standards also contain this information and as standards are revised the GTB doesn't always match to the new updates.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018
20-day formal comment period with ballot	October 2018
15-day formal comment period with additional ballot	November 2018

Anticipated Actions	Date
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms

Cyber Security Incident:
A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that 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.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-6

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 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 Reportable Cyber Security Incident; 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.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

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].*

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.*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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),[1] 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:
None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)	the "Applicable Systems" column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days	Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity	Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their	"Applicable Systems" column. (R4)	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ final draft of proposed standard for formal ~~1~~5-day ~~comment~~ final ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018
20-day formal comment period with ballot	October 2018
15-day formal comment period with additional ballot	November 2018

Anticipated Actions	Date
~~15-day formal comment period with additional ballot~~	~~November 2018~~
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms:

Cyber Security Incident:

A malicious act or suspicious event that:

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

Reportable Cyber Security Incident:

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~~(s)~~ of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System~~s~~ of a high or medium impact BES Cyber System.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-6

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] ~~]~~ that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

B. Requirements and Measures

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].*

M1. 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*.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes ~~to~~ : 1.2.1 That include ~~Establish~~ criteria to evaluate and define attempts to compromise; 1.2.2 To d~~D~~etermine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident~~;~~ or • ~~Only~~ 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 p~~P~~rovide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be ~~only~~an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*

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*.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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 thisthe 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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that -is determined to be only an attempt to compromise a system identified in the "Applicable Systems" column.

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].*

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.*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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),[1] or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was ~~only~~ 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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 ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was ~~only~~ an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include ~~to establish~~ criteria to evaluate and define attempts to compromise. (1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	calendar months between tests of the plan(s). (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified	less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role	120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was ~~only~~ an attempt to compromise, as determined by applying the criteria from Requirement R1,	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to ~~Requirement R4,~~ Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to	Part 1.2.1, a system identified in the "Applicable Systems" column. (R4)	timelines pursuant to ~~Requirement R4,~~ Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Requirement R4,~~ Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to ~~Requirement R4,~~ Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	August 9, 2018
SAR posted for comment	August 10 – September 10, 2018
20-day formal comment period with ballot	October 2018
15-day formal comment period with additional ballot	November 2018

Anticipated Actions	Date
5-day final ballot	January 2019
Board adoption	February 2019

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Proposed Modified Terms

Cyber Security Incident:
A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, ~~C~~compromises~~,~~ or ~~was an~~ attempts 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~~ attempts to disrupt~~,~~ the operation of a BES Cyber System.

Reportable Cyber Security Incident:
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.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~5~~6

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System or~~ Remedial Action Scheme where the ~~Special Protection System or~~ Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5~~ identification and categorization processes.

5. Effective Dates:

~~1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~**6.**~~ See Implementation Plan for CIP-008-6.

6. Background:

Standard CIP-008~~-5~~ exists as part of a suite of CIP Standards related to cyber security. CIP-002~~-5~~ requires the initial identification and categorization of BES Cyber Systems. CIP-003~~-5~~, CIP-004~~-5~~, CIP-005~~-5~~, CIP-006~~-5~~, CIP-007~~-5~~, CIP-008~~-5~~, CIP-009~~-5~~, CIP-010~~-1~~, and CIP-011~~-1~~ require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc~~.~~] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~its documented processes, but ~~they~~ must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it ~~makes sense and~~ is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact

and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002~~-5~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002~~-5~~ identification and categorization processes.

B. Requirements and Measures

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-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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~~; or • An attempt to compromise, as determined by applying the ~~Electricity Sector Information Sharing~~criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and ~~Analysis Center (ES-ISAC), unless prohibited by law. Initial~~ 1.2.3 To provide 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~~	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents ~~and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).~~ or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

CIP-008-~~5~~6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		~~Incident.~~per Requirement R4.	
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and -Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-~~5~~6 Table R2 – Cyber Security Incident Response Plan Implementation and -Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents- and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

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-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

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-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

CIP-008-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-~~5~~6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

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),[1] 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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

[1] 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).

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
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 non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:
None

2. ~~2.~~ Table of Compliance Elements

~~R~~ #	Time Horizon	VRF	Violation Severity Levels (CIP-008-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	~~Lower~~	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents~~.~~ or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (1.2) ~~OR~~ ~~The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)~~
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months between tests of the plan(s). (2.1)	months between tests of the plan(s). (2.1)	months between tests of the plan(s). (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (2.2)	between tests of the plan(s). (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role	incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the	response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

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.~~

~~The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.~~

~~Requirement R2:~~

~~Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.~~

~~Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. 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."~~

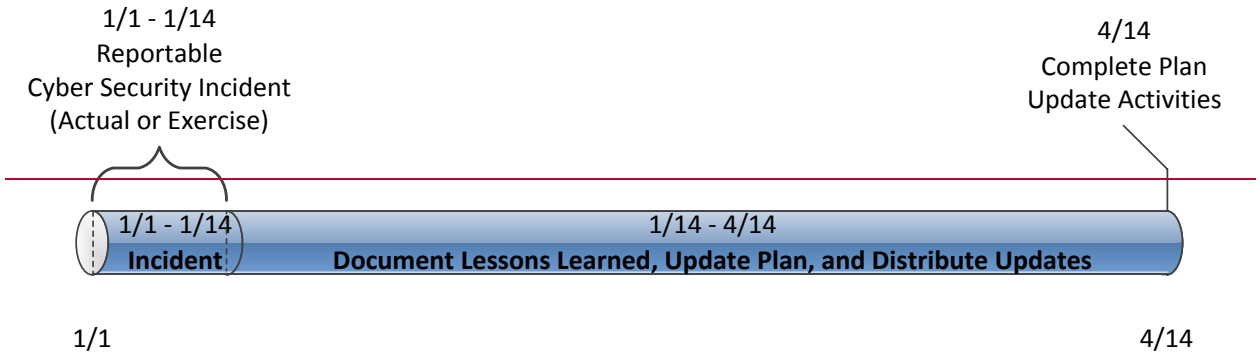
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation 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*. 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.~~

~~Requirement R3:~~

~~This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.~~

~~The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.~~



~~Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. 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.~~

~~The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.~~

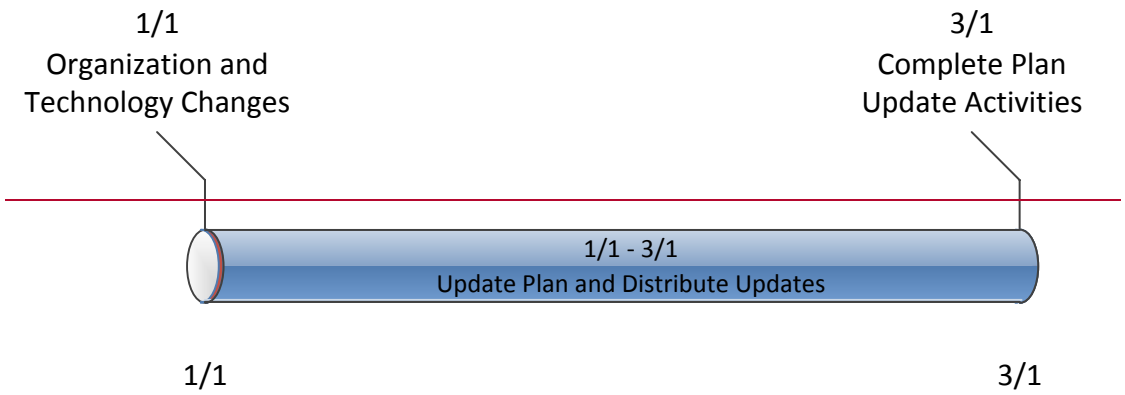


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. 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.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard and Definitions

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident

Requested Retirements

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident (currently effective definition)
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident (currently effective definition)

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of this project is to address the directives that FERC issued in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the Reliable Operation of the Bulk

Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the four elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;
2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center (NCCIC)[1].

Effective Date

Reliability Standard CIP-008-6
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.

Revised Definitions for Cyber Security Incident and Reportable Cyber Security Incident
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.

[1] 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).

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.

Retirement Date

Reliability Standard CIP-008-5
Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Currently Effective Definitions for Cyber Security Incident and Reportable Cyber Security Incident
The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

Applicable Standard and Definitions

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident

Requested Retirements

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident (currently effective definition)
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident (currently effective definition)

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

~~New Terms in the NERC Glossary of Terms~~

~~This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed~~

~~standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the *Glossary of Terms Used in NERC Reliability Standards*.~~

~~**Proposed Modified Definitions:**~~

~~Cyber Security Incident:~~

~~A malicious act or suspicious event that:~~

- ~~For a high or medium impact BES Cyber System, c~~Compromises, or was an attempt to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; ~~or~~
- ~~Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.~~

~~Reportable Cyber Security Incident:~~

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

- ~~A BES Cyber System that performs one or more reliability tasks of a functional entity;~~
- ~~Electronic Security Perimeter(s); or~~
- ~~Electronic Access Control or Monitoring Systems.~~

~~**Proposed Retirements of Approved Definitions:**~~

~~Cyber Security Incident:~~

~~A malicious act or suspicious event that:~~

- ~~Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,~~
- ~~Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.~~

~~Reportable Cyber Security Incident:~~

~~A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.~~

Background

The purpose of this project is to address the directives that FERC issued i~~ by FERC i~~n Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the Reliable Operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "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)." (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the four~~4~~ elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS;

2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the United States National Cybersecurity and Communications Integration Center (NCCIC);[1] ~~the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)~~.

Effective Date

Reliability Standard CIP-008-6

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.

Revised Definitions for Cyber Security Incident and Reportable Cyber Security Incident

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.

Retirement Date

Reliability Standard CIP-008-5

[1] 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).

Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

Currently Effective Definitions for Cyber Security Incident and Reportable Cyber Security Incident

The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-008-6. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-008-6, Requirement R1
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R1
The justification is provided on the following pages.

VRF Justification for CIP-008-6, Requirement R2
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R2
The VSL did not substantively change from the previously FERC-approved CIP-008-5 Reliability Standard. Only minor revisions were made.

VRF Justification for CIP-008-6, Requirement R3
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R3
The VSL did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VRF Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSL Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSLs for CIP-008-6, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (1.2)

		criteria to evaluate and define attempts to compromise. (1.2)	

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from FERC-approved CIP-008-5 and add two VSLs to the High and Severe categories to reflect new subparts 1.2.1 and 1.2.3. The two new VSLs are similar to currently-approved VSLs. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The proposed VRF is consistent among other FERC approved VRF's within the standard.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The team relied on NERC's definition of lower risk requirement.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1. (4.1)		successors, of a Reportable Cyber Security Incident. (R4)	

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in CIP-008-6. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification for CIP-008-6, Requirement R1
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R1
The justification is provided on the following pages.

VRF Justification for CIP-008-6, Requirement R2
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R2
The VSL did not substantively change from the previously FERC-approved CIP-008-5 Reliability Standard. Only minor revisions were made.

VRF Justification for CIP-008-6, Requirement R3
The VRF did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VSL Justification for CIP-008-6, Requirement R3
The VSL did not change from the previously FERC-approved CIP-008-5 Reliability Standard.

VRF Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSL Justification for CIP-008-6, Requirement R4
The justification is provided on the following pages.

VSLs for CIP-008-6, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include ~~to establish~~ criteria to evaluate and	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was ~~only~~ an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (1.2)

		define attempts to compromise. (1.2)	

VSL Justifications for CIP-008-6, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from FERC-approved CIP-008-5 and add two VSLs to the High and Severe categories to reflect new subparts 1.2.1 and 1.2.3. The two new VSLs are similar to currently-approved VSLs. As a result, the proposed VSLs do not lower the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Lower is being proposed for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The proposed VRF is consistent among other FERC approved VRF's within the standard.

VRF Justifications for CIP-008-6, Requirement R4	
Proposed VRF	**Lower**
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The team relied on NERC's definition of lower risk requirement.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to ~~Requirement R4,~~ Part 4.2. (4.2)	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber Security Incident that was ~~only~~ 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. (R4)	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to ~~Requirement R4,~~ Part 4.2. (4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)

VSLs for CIP-008-6, Requirement R4			
Lower	**Moderate**	**High**	**Severe**
OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to ~~Requirement R4,~~ Part 4.1. (4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was ~~only~~ an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to ~~Requirement R4,~~ Part 4.1. (4.1)		successors, of a Reportable Cyber Security Incident. (R4)	

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-008-6, Requirement R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Incident Report

Technical Rationale and Justification for Reliability Standard CIP-008-6

January 2019

RELIABILITY | ACCOUNTABILITY



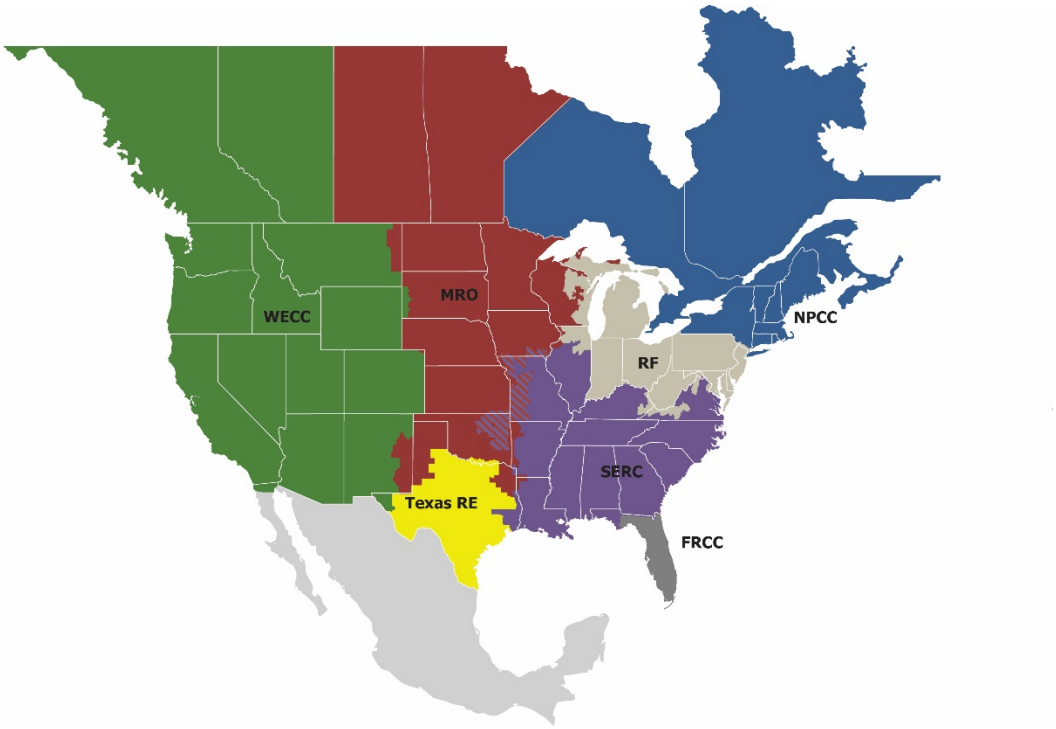

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards 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 and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

[1] 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).

New and Modified Terms Used in NERC Reliability Standards

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident

A Cyber Security Incident that 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 Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for "A BES Cyber System that performs one or more reliability tasks of a functional entity" to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

New and Modified Terms Used in NERC Reliability Standards

EACMS

The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "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 the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "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."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

Requirement R4

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Requirement R4

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-008-5 standard to preserve any historical references.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:
This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. 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*.

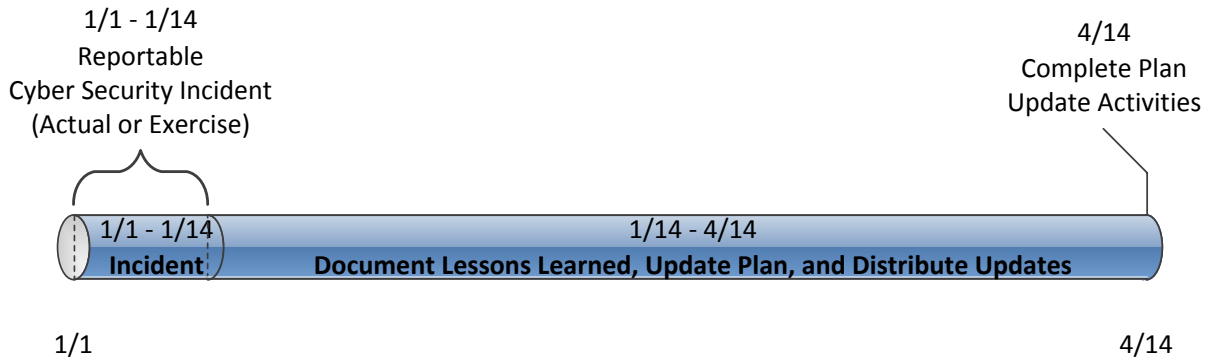
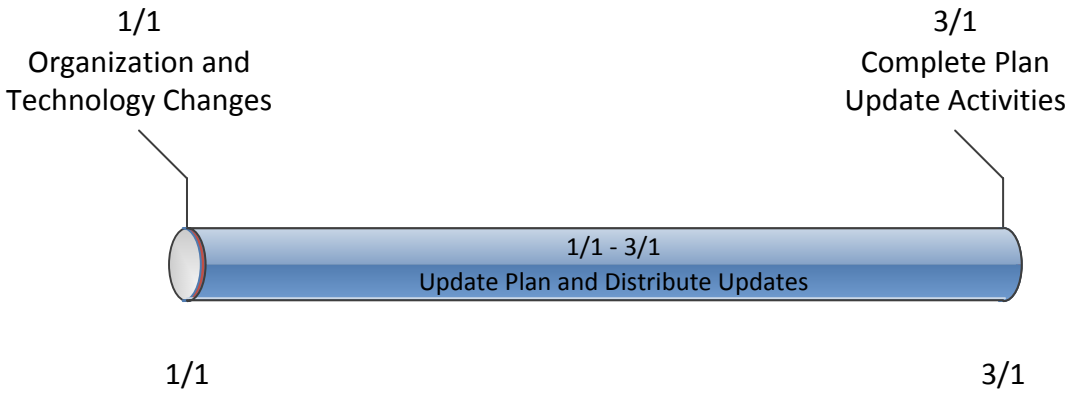


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 2019 - DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Incident Reporting and Response Planning

Implementation Guidance for CIP-008-6

RELIABILITY | ACCOUNTABILITY




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

Table of Contents

List of Figures

Introduction

The Standards Project 2018-02 – Modifications to CIP-008 Standard Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-008-6. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1]

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP- 008-6.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 848 on July 19, 2018, calling for modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.[2] The Commission directed the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the Reliability Standards 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).[3]

The Commission's directive consisted of four elements intended to augment the current Cyber Security Incident reporting requirement: (1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) now known as NCCIC[4]. Further, NERC must file an annual, public, and anonymized summary of the reports with the Commission.

The minimum attributes to be reported should 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.

The Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require responsible entities to meet the directives set forth in the Commission's Order No. 848.

---

[1] NERC's Compliance Guidance Policy

[2] 16 U.S.C. 824o(d)(5). The NERC Glossary of Terms Used in NERC Reliability Standards (June 12, 2018) (NERC Glossary) defines a Cyber Security Incident as "A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."

[3] The NERC Glossary defines "ESP" as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." The NERC Glossary defines "EACMS" as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

[4] The DHS ICS-CERT underwent a reorganization and rebranding effort and is now known as the National Cybersecurity and Communications Integration Center (NCCIC).

Definitions

CIP-008-6 has two related definitions, as well as language for "attempts to compromise" that is specific to CIP-008-6 within Requirement R1 Part 1.2.2. Cyber Security Incidents are not reportable until the Responsible Entity determines one rises to the level of a Reportable Cyber Security Incident or meets the Responsible Entity's established criteria for attempts to compromise pursuant to Requirement R1 Part 1.2.1 and 1.2.2. When these thresholds are reached reporting to both E-ISAC and NCCIC (Formerly DHS's ICS-CERT) is required. These definitions and requirement language are cited below for reference when reading the implementation guidance that follows.

Cyber Security Incident:
A malicious act or suspicious event that:

- For high or medium Impact BES Cyber Systems, compromises, or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Cyber Security Incident:
A Cyber Security Incident that 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.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications		
Part	**Applicable Systems**	**Requirements**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 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 Reportable Cyber Security Incident, 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.

The determination of reportability for compromises or disruptions (by definition), or for attempts to compromise (pursuant to the requirement language), becomes a function of applying criteria that builds upon the parent definition of Cyber Security Incident.

A color code that progresses from no reportability to greatest reportability is used in Figure 1.

GREEN	YELLOW	ORANGE	RED
non-reportable events/activity, or determination not made	is Cyber Security Incident, reportable determination not made	is determined reportable attempt to compromise an Applicable System	is determined Reportable Cyber Security Incident

The below Venn diagram illustrates the relationships between the elements of each definition, and the Requirement R1 Part 1.2.2 requirement language. In this example, one potential option could be to leverage the EACMS function descriptors noted in FERC Order 848 Paragraph 54 as criteria. This could serve as an approach to assess operational impact and/or functionality of cybersecurity controls that cause a Cyber Security Incident to rise to either level of reportability:

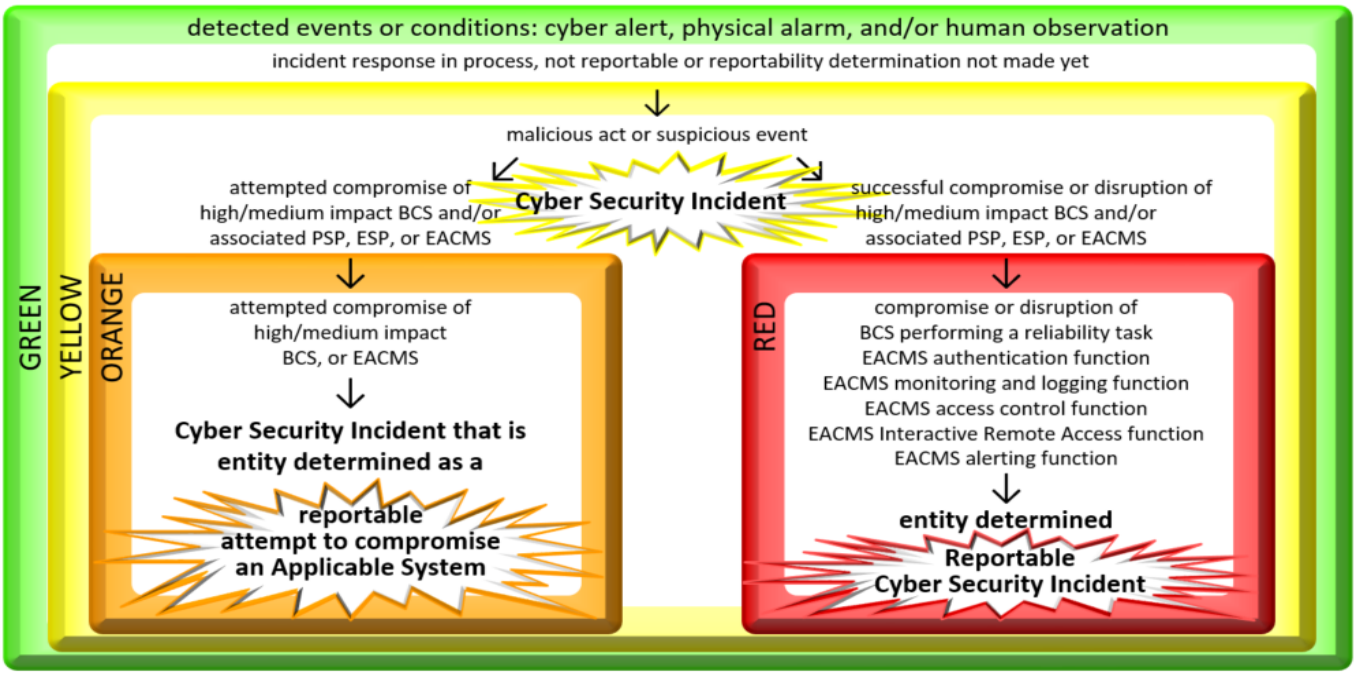


Figure 1 Relationship of Cyber Security Incidents

As shown in the above diagram, there is a progression from identification through assessment and response before a detected event or condition elevates to a reportable level.

First, the Registered Entity must determine the condition meets the criteria for a Cyber Security Incident.

Once the response and assessment has led to a Registered Entity's determination that events or conditions meet the definition of Cyber Security Incident, additional evaluation occurs to determine if established criteria or thresholds have been met for the Registered Entity to determine the Cyber Security Incident qualifies for one of the two reportable conditions:

1. Reportable Cyber Security Incident.
2. An attempt to compromise one or more systems identified in the "Applicable Systems" column for Requirement R4 Part 4.2 (pursuant to Responsible Entity processes and established attempt criteria documented in accordance with Requirement R1 Part 1.2)

Once the response and investigation has led to a Registered Entity's determination that the Cyber Security Incident has targeted or impacted the BCS performing reliability tasks and/or cybersecurity functions of the Applicable Systems, associated Cyber Assets, and/or perimeters, the notification and reporting timeframes and obligations begin. Note: Initial (or preliminary) notification is needed within the specified timeframe after this determination, even if required attributes (functional impact, level or intrusion, attack vector) are not yet known.

Once this initial notification is made, if all attributes were known, they should have been included in the initial notification and the reporting obligation ends.

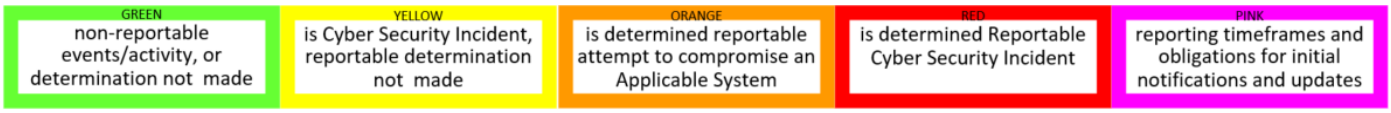
If all attributes were not known by the time the initial notification had to be made, the update timeframes trigger from the time the next attribute(s) is determined to be learned/known.

A Registered Entity's reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC, either during the initial notification or subsequently through one or more updates made commensurate with the reporting timeframes.

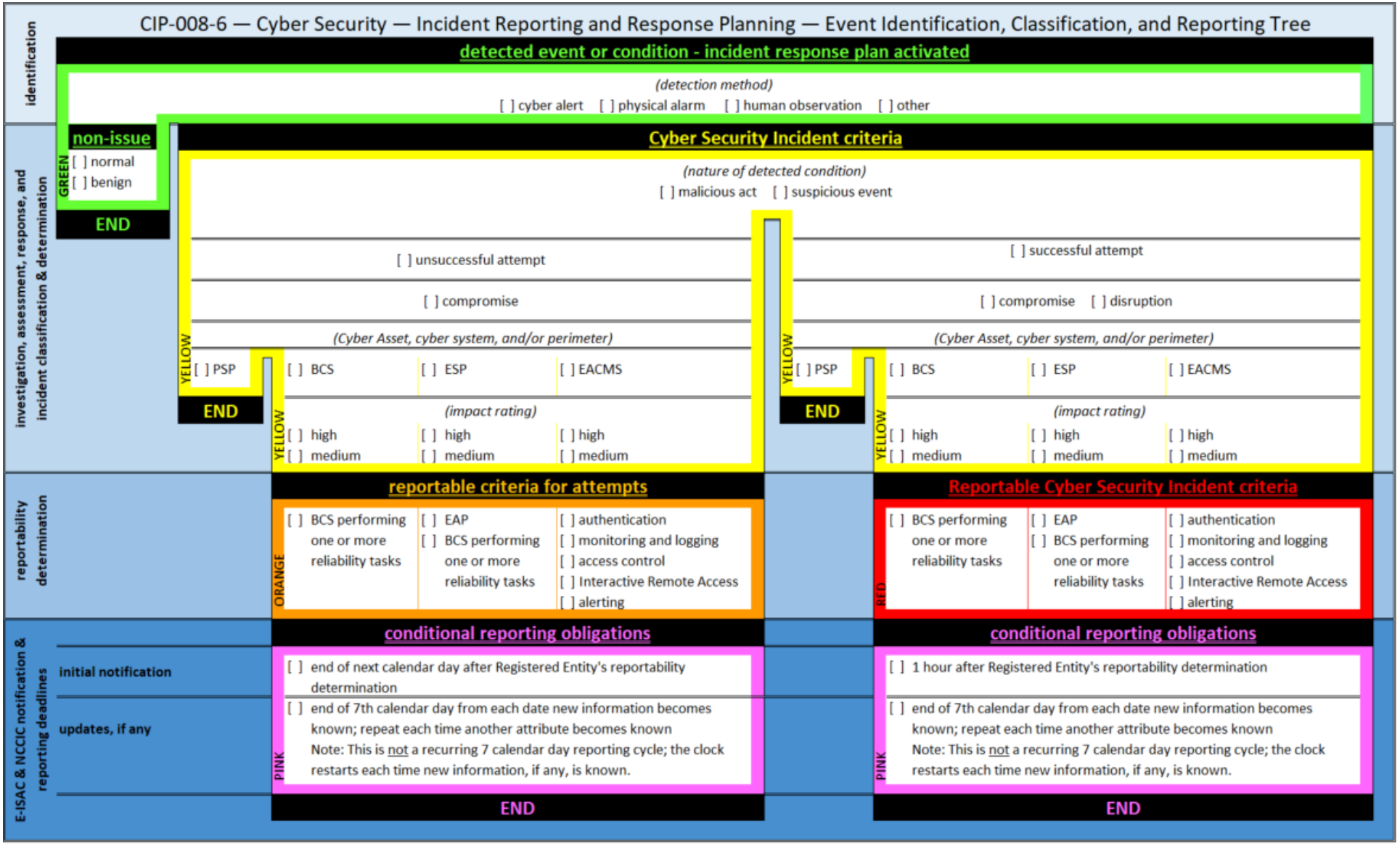
Determination and Classification of Cyber Security Incidents

Registered Entities may want to consider developing tools illustrating established process criteria that must be met, by definition, as well as the impacted/targeted operational task/cybersecurity functions considered to reach each incident classification and reporting threshold. The below decision tree is one potential approach Registered Entities could employ as a tool to assess events and make the Registered Entity determinations according to process(es) and established criteria documented pursuant to Requirement R1 Parts 1.1 and 1.2. Note: Where the term "criteria" is used in the optional tool examples, it is intended to serve as a section the entity may tailor to match the criteria they have included in their process(es). What is included in this guidance is not prescriptive and only one potential approach.

A similar color code to the diagram depicting the relationships between definitions and requirement language has been used to illustrate a progression from no reportability to greatest reportability inclusive of the respective reporting obligations and timeframes for initial notifications and updates for Figure 2 and Figure 3.



The blue shading in Figure 2 simply represents the distinction between phases in the incident response process as analysis and investigative actions occur and information unfolds.



*Where 'calendar day' is used, the 'end' of the day = 11:59 PM local time of that day.

** Where 'determination' is used, this refers to the Registered Entity's determination.

Figure 2 Potential Approach Tool

A second potential approach could be a flow diagram illustrating an entity's criteria and determination process as depicted in the example below:

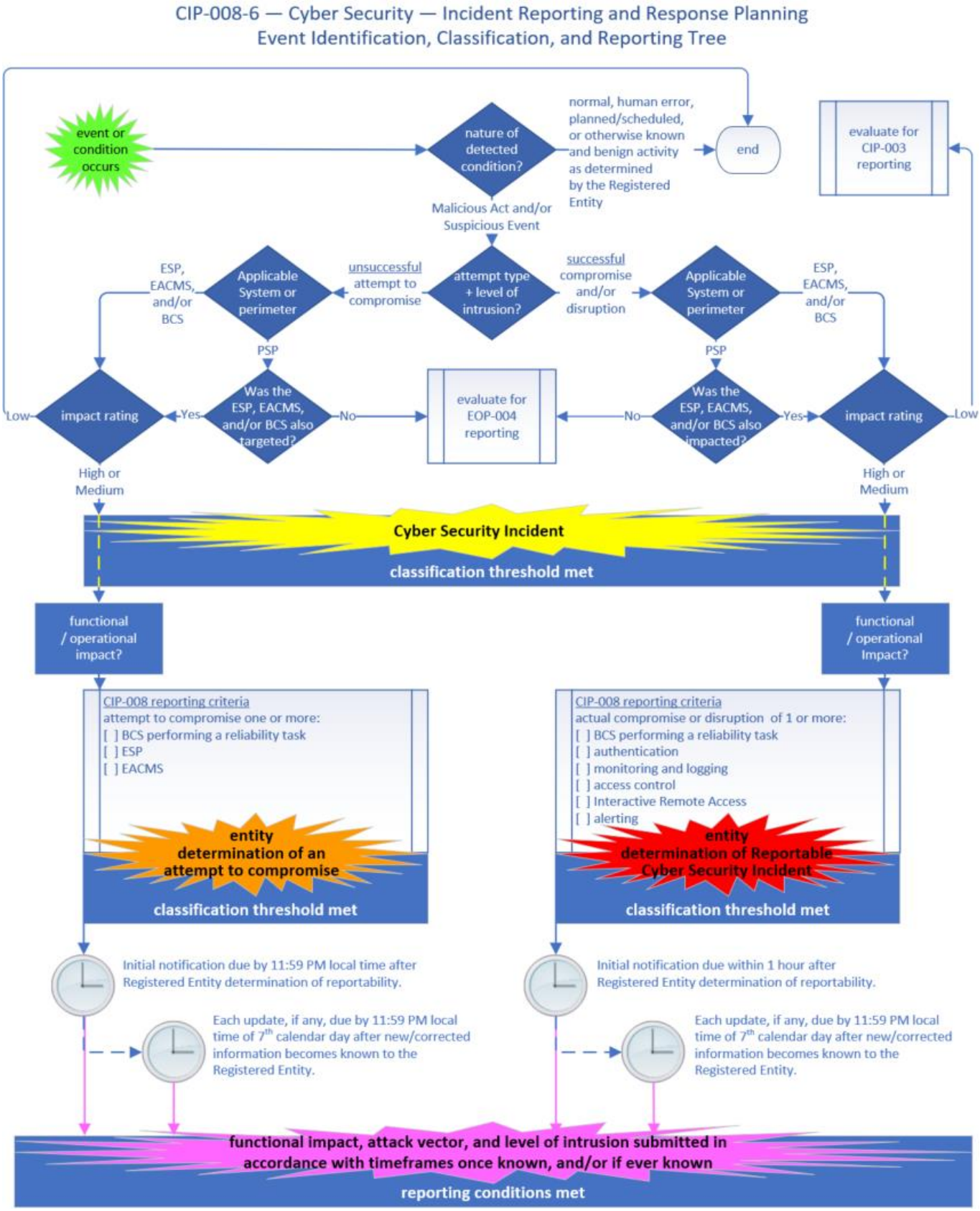


Figure 3: Flow Diagram for Cyber Security Incidents

Example of a Cyber Incident Classification Process

Entities may use a risk analysis-based method for the classification of cyber incidents and determination of Cyber Security Incidents, Reportable Cyber Security Incidents or, Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The risk analysis-based approach allows entities the flexibility to customize the appropriate response actions for their situation without being administratively burdened by a one size fits all solution. Entities also have the flexibility to incorporate their existing incident management processes which may already define how they classify and determine cyber incidents.

A risk-based approach considers the number of cyber security related event occurrences, the probability that the events will have an impact on their facilities, and severity of the impact of the event. This allows the entity to decide when cyber events should be investigated as cyber incidents, the classification of cyber incidents and the determination of when a cyber incident should be reported; either as part of a voluntary action, as part of a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

Entities should also consider that appropriate reporting of cyber incidents helps other entities in similar situations. The reporting of the details of an incident serves to alert other entities so they may increase their vigilance and take timely preventive or mitigating actions. All entities stand to benefit from such shared information in the long run.

As an example, a typical infrastructure installation is depicted in Figure below.

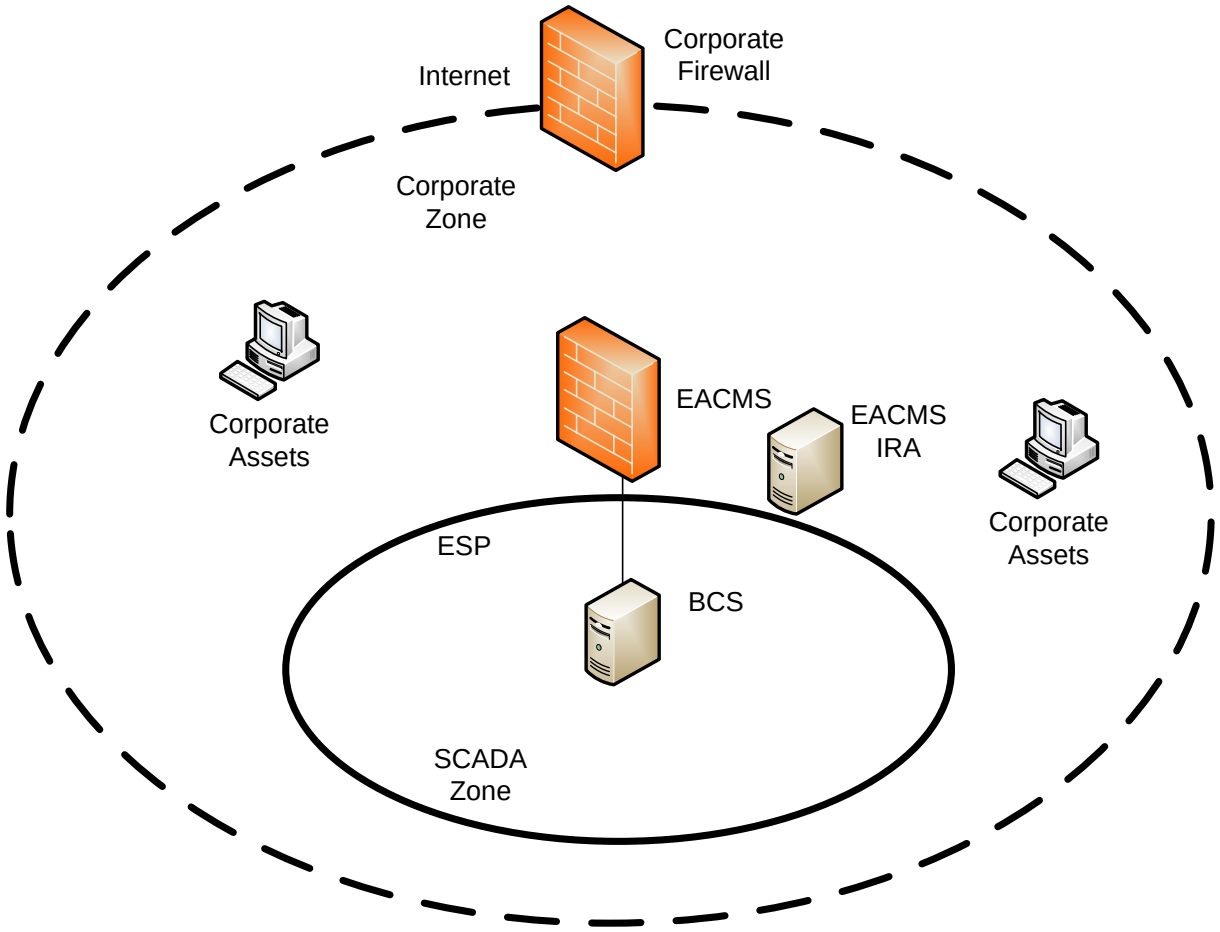


Figure 4 Typical Infrastructure

- A SCADA security zone consists of BES Cyber System (BCS), behind an Electronic Security Perimeter (ESP). The Electronic Access Point (EAP) is an interface of the SCADA firewall which is an Electronic Access Control or Monitoring System (EACMS).
- A Corporate security zone consists of regular corporate assets and other EACMS such as Intermediate Systems with Interactive Remote Access (IRA). A corporate firewall protects the corporate assets against intrusions from the Internet. The SCADA security zone is nested inside the corporate security zone.

Sample Classification Schema

A risk analysis could produce the incident categories below:

- Regular cyber events that represent a normal level of events where no further investigation is required such as random port-scans.
- Low risk incidents may be cyber events that become cyber incidents because they are beyond the normal level of events and require some type of investigation. Cyber incidents that are blocked at a firewall and found not to be malicious or suspicious could fall into this category.
- Medium risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and required mitigation activities.

  Note that while these cyber incidents were malicious or suspicious, they might not meet the definition of a Cyber Security Incident because the entity investigated and determined that the target was not a BCS, ESP, PSP or EACMS.

  For example, a corporate asset infected with well-known corporate malware and, as a result, is scanning the network to find other corporate assets. Although this activity is also being seen at the SCADA firewall (EACMS), the entity investigated and determined that this activity was not a Cyber Security Incident.
- High risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and did meet the definition of Cyber Security Incidents. For example, malicious malware on a corporate asset that repeatedly attempts to log into a SCADA IRA Intermediate System but is unsuccessful. This would be a Cyber Security Incident and should also fall into the entity's definition of a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part with the target being an EACMS (SCADA IRA Intermediate System).
- Severe risk incidents may be those Cyber Security Incidents that involves successful compromise of an ESP or EACMS and hence meet the criteria for Reportable Cyber Security Incident. These may also escalate into Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as the BCS.
- Emergency risk incidents may be those Cyber Security Incidents that compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity. These incidents may represent an immediate threat to BES reliability and may require emergency actions such as external assistance.

These incident categories can be mapped into a standard incident classification and reporting schema like the NCCIC Cyber Incident Scoring System[5]. This is a common schema used by the United States Federal Cybersecurity Centers for describing the severity of cyber incidents and is available to industry to leverage.

Utilizing the NCCIC schema as a basis for identification and classification of Cyber Security Incidents could be adapted to produce the schema below for application to CIP-008-6:

	General Definition	Consequences
Level 5 Emergency Black	A cyber incident that investigation found was a Cyber Security Incident that has compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity.	Incidents that result in imminent threat to public safety and BES reliability. A Reportable Cyber Security Incident involving a compromise or disruption of a BCS that performs one or more reliability tasks of a functional entity.
Level 4 Severe Red	A cyber incident that investigation found was a Cyber Security Incident involving a compromise or disruption of an ESP or EACMS; OR A cyber incident that investigation found was a Cyber Security Incident that attempted to compromise a BCS.	Cyber Security Incidents that have the potential to result in a threat to public safety and BES reliability if malicious or suspicious activity continues or escalates. Immediate mitigation is required. A Reportable Cyber Security Incident involving a compromise or disruption of a EACMS or ESP OR A Cyber Security Incident that must be reported as an attempt to compromise or disrupt a BCS
Level 3 High Orange	A cyber incident that investigation found met the entity's defined criteria for a Cyber Security Incident that attempted to compromise or disrupt an EACMS or ESP	An attempt to compromise an EACMS does not result in a threat to public safety or BES reliability, but still requires mitigation. A Cyber Security Incident that must be reported as an attempt to compromise or disrupt an EACMS
Level 2 Medium Yellow	A cyber incident that investigation found was malicious or suspicious but was not a Cyber Security Incident because it did not target an Applicable System or perimeter.	A cyber incident that does not represent a threat to public safety or BES reliability, even though it is malicious or suspicious and required mitigation.
Level 1 Low Green	A cyber incident that investigation found was not malicious or suspicious.	A cyber incident that does not represent a threat to public safety.
Level 0 Baseline White	Inconsequential cyber events.	Cyber events that require no investigation and are not cyber incidents. These do not represent a threat to public safety.

Figure 5 Example of Classification Schema

Reliability tasks may be those tasks that a Responsible Entity determines are associated with the BES Reliability Operating Services (BROS) listed in the NERC Functional Model.

[5] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Examples of the use of the Sample Classification Schema

Some examples of the use of the classification schema are listed below. The event number corresponds to the events depicted in the subsequent figures. The color code defined in the sample schema in Figure 5 is carried through Figures 6- 8.

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
External firewall scan (N1 – no color)	External IPS log Review of F/W log	External IPS Corporate F/W rules	No	No	No	Determined by entity as regular background activity
Corporate Zone internal scan by non-malicious source (existing network monitoring Tool) (N2 - no color)	Corporate IPS Review of EACMS – IRA host F/W Log (CIP-007 R4)	Corporate IPS EACMS IRA Host F/W	No	No	No	Determined by entity as regular background activity – previously investigated and determined to be known source

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone internal scan by unknown source (N3 - green)	Corporate IPS Review of EACMS IRA host F/W Log	Corporate IPS IRA EACMS Host F/W	Yes	No	No	Investigation found new network monitoring tool. Added to regular background activity.
Corporate Zone Internal scan by unknown source (N4 - yellow)	Corporate IPS Corporate Antivirus Review of EACMS IRA host F/W Log Review of EACMS SCADA F/W Log	Corporate IPS IRA EACMS Host F/W Corporate Anti-virus SCADA F/W EACMS	Yes	No	No	Investigation by entity determined malware in Corporate zone was targeting other corporate assets and not specifically the Applicable Systems. (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by EACMS IRA login attempts (N5 - orange)	Corporate IPS Review of EACMS IRA host F/W Log Review of EACMS IRA failed Logins (CIP-007 R4)	Corporate IPS EACMS host F/W EACMS login 2 factor	Yes	Yes EACMS – IRA targeted	Yes Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Investigation found malware in Corporate zone was an attempt to compromise one or more Applicable Systems - IRA Intermediate System - EACMS (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by successful EACMS IRA login and attempted BCS logins (N6 - red)	SCADA IPS log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS failed Logins (CIP-007 R4)	SCADA IPS (CIP-005 R1.5) BCS user/ password login	Yes	Yes	Yes EACMS – IRA host compromised or disrupted Reportable Cyber Security Incident BCS host failed logins Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as BCS	Investigation found malware compromised or disrupted EACMS IRA. Attempt to compromise a BCS. (via the entity's criteria to evaluate and define attempts to compromise)

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
BCS – SCADA system failure following Corporate Zone Internal scan by unknown source, successful EACMS IRA login and successful BCS login (N7 - black)	SCADA system log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS Logins (CIP-007 R4)	None	Yes	Yes	Yes Comprise or disruption of a BCS performing one or more reliability tasks of a functional entity Reportable Cyber Security Incident	Investigation found malware compromised a BCS performing one or reliability tasks of a functional entity

Figure 6 Examples of the Use of the Classification Schema

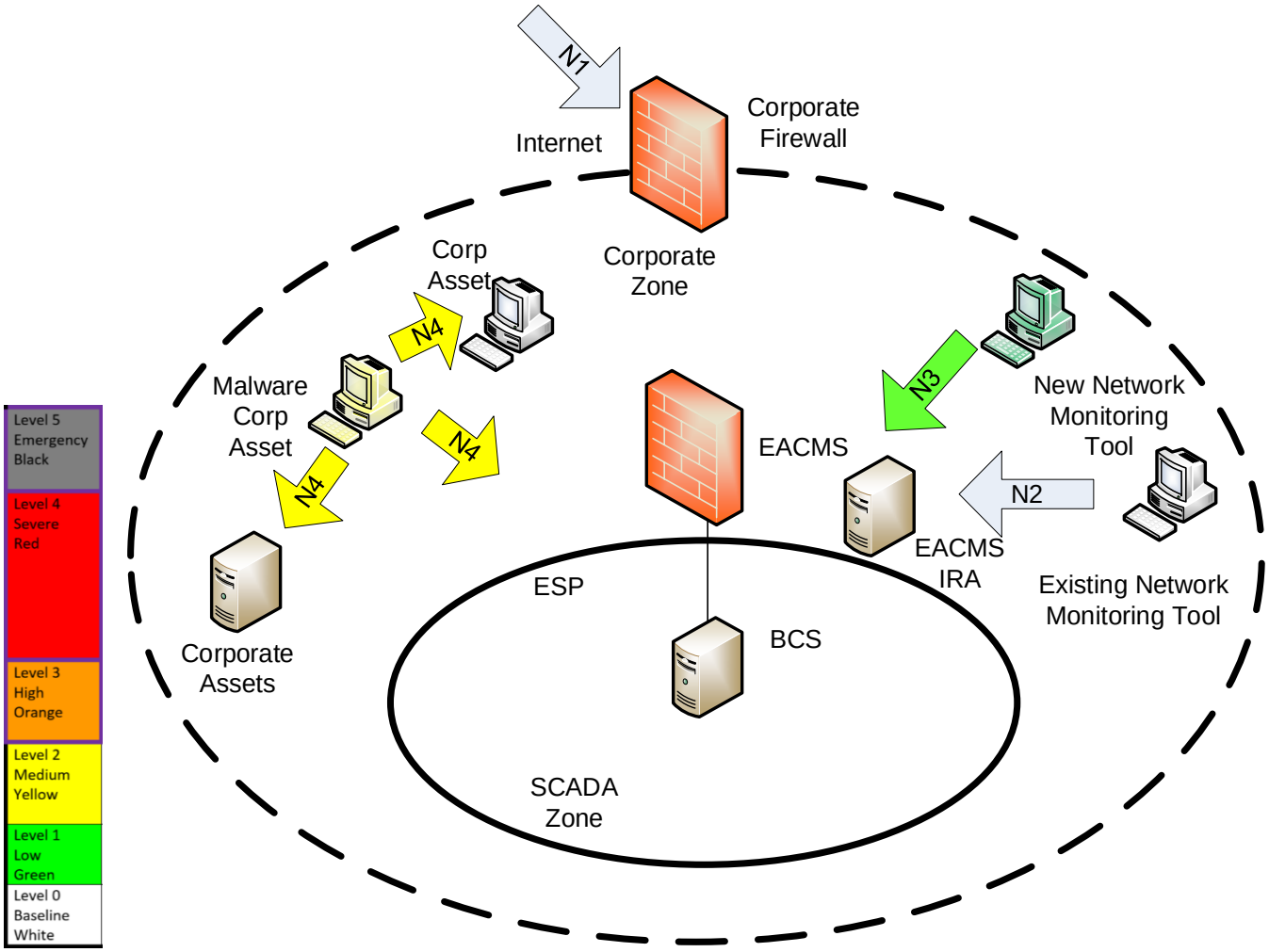


Figure 7 Examples of Non-Reportable Cyber Incidents

The figure above depicts examples of non-reportable cyber incidents using the sample classification schema and examples in Figure 6.

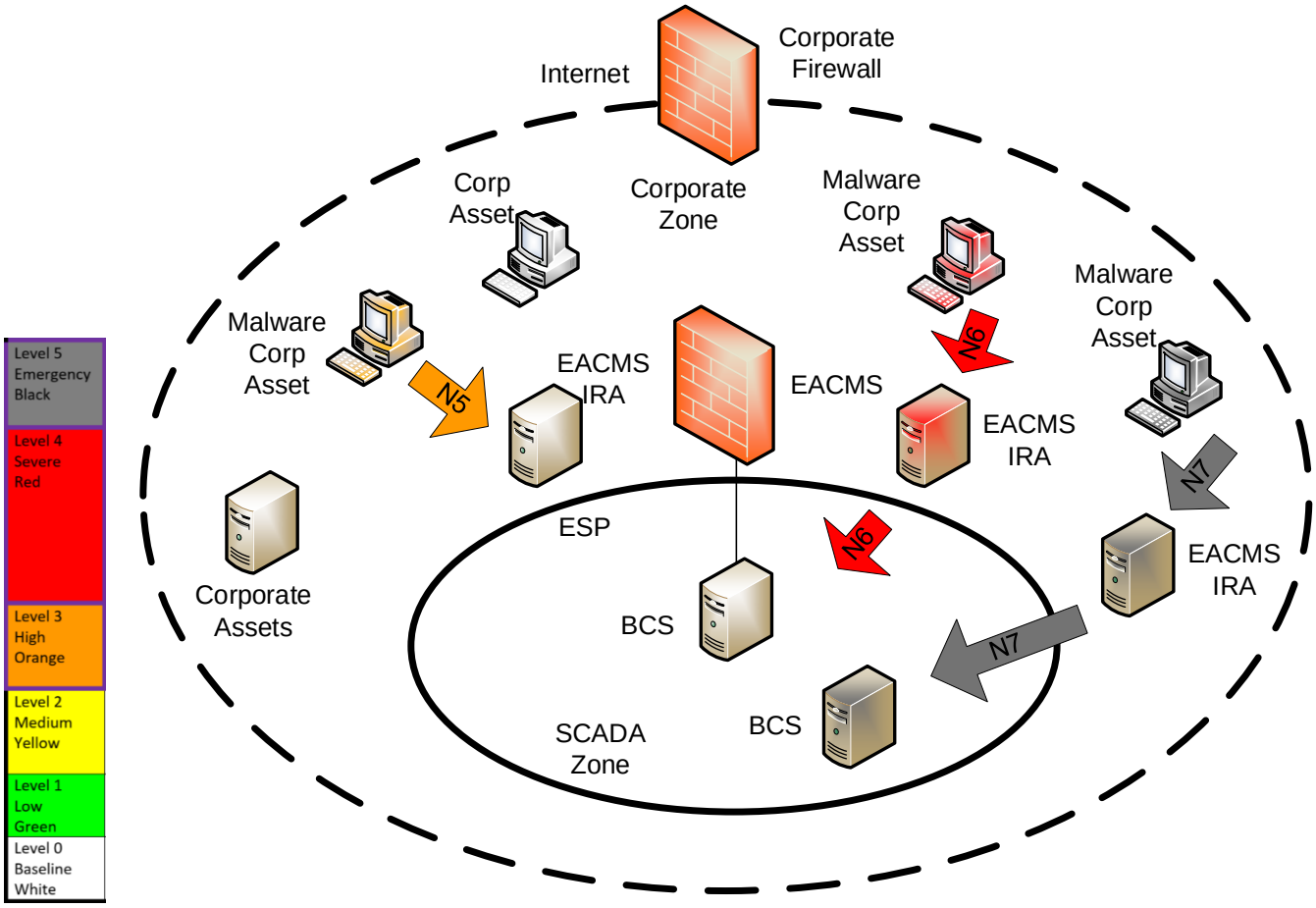


Figure 8 Examples of Reportable Cyber Security Incidents or attempt to compromise one or more applicable systems

The figure above depicts examples of Reportable Cyber Security Incidents or attempts to compromise one or more systems identified in the "Applicable Systems" column for the Part using the sample classification schema and examples in Figure 6.

Attempts to Compromise and Cyber Security Incidents

Registered Entities should evaluate and determine what is normal within their environment to help scope and define what constitutes 'an attempt to compromise' in the context of CIP-008, and should document established criteria within the entity processes. This can help Subject Matter Experts (SMEs) identify deviations from normal, and assist a Registered Entity in timely and effective incident determination, response, and vital information sharing.

Entities are encouraged to explore solutions designed to take the guess work out of the process without being overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs. Entities may want to consider options like a decision tree or a checklist for SMEs to apply defined criteria used to determine reportability.

As an example, an entity could define an "attempt to compromise" as an act with malicious intent to gain access or to cause harm to normal operation of a Cyber Asset in the "Applicable Systems" column. Using this sample definition, some criteria could be:

1. Actions that are **not** an attempt to compromise an applicable Cyber Asset/System electronically are:
   a. An entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence that is performed expected on demand or on an approved periodic schedule.
   b. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic, but it does not have malicious intent.
   c. Attempts to access a Cyber Asset by an authorized user that have been determined to fail due to human error.
2. Actions that **are** an attempt to compromise an applicable Cyber Asset/System electronically are:
   a. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management nor process(es). This could be from an entity's own equipment due to an upstream compromise or malware.
   b. Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.
   c. Attempts to escalate privileges on a Cyber Asset by an authorized user that has been determined to fail due to not being authorized for that privilege level.

Registered Entities may also want to evaluate system architecture for ways to limit exposure for 'attempts to compromise'. Techniques like the implementation of security zones and/or network segmentation can minimize the level of traffic that can get to applicable Cyber Assets and help minimize the attack surface.

Registered Entities with implementations that involve an EACMS containing both an Electronic Access Point (EAP) and a public internet facing interface are strongly encouraged to change this configuration in favor of architectures that offer layers of safeguards and a defense in depth approach.

Similarly, Registered Entities with implementations involving an EACMS containing both an EAP and a corporate facing interface to their business networks may also want to consider options to re-architect to reduce cyber events from the corporate environment such as broadcast traffic from causing extra administrative workload.

A color code that progresses from no reportability to greatest reportability is used in Figure 9.

Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

The table below contains examples of various degrees of events or conditions at varied levels of determination:

Event	Normal or Benign		Malicious / Confirmed Suspicious	
PSP breach	• Unauthorized user compromises the PSP to steal copper and the Registered Entity determines cybersecurity controls were not targeted and remain in place.	GREEN	• Unauthorized user breaks into a Substation control house (**CIP-006-6 R1.5 activates BES Cyber Security Incident response plan within 15 minutes of detection.**)	GREEN
			• Unauthorized user breaks into a Substation control house and inserts unauthorized Removable Media into an EACMS or BCS and the Registered Entity determines no interaction between the USB and the EACMS or BCS occurred. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
	• An equipment operator loses control of a backhoe and crashes into a control house, breaching the PSP and the Registered Entity determines it was accidental; cybersecurity controls were not targeted and remain in place.	GREEN	• Registered Entity determines the unauthorized Removable Media contains malware (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• Registered Entity determines the malware has harvested the credentials of a BCS, gained unauthorized access and disrupted a reliability task. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED
Port Scanning	• Registered Entity owned monitoring tool that runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at the expected time.	GREEN	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at an unexpected time and the Registered Entity has determined this as suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
	• A Registered Entity performs a port scan of an EACMS or BCS during a scheduled Cyber Vulnerability Assessment activity.	GREEN	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it is targeting specific ports relevant to the BCS. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it gained unauthorized access to the EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED

Event	Normal or Benign		Malicious / Confirmed Suspicious	
Detected malware	• A corporate machine infected by a known Windows-specific vulnerability is scanning all local hosts including non-Windows-based EACMS or BCS and is determined by the Registered Entity to be an SMB exploit applicable to only Windows-based machines.	GREEN	• An infected corporate machine is scanning all local hosts including an EACMS or BCS for well-known ports and determined to be a suspicious event by the Registered Entity. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)	YELLOW
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and has attempted to gain unauthorized access to the EACMS or BCS. (**determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)	ORANGE
			• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and exploited/compromised specified ICS ports that perform command and control functions of a BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)	RED
Login activity	• Authorized user exceeded the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login attempts against an EACMS or BCS and the Registered Entity confirmed the user incorrectly entered his/her password after performing annual password changes.	GREEN	• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity investigates that activity as a Cyber Security Incident because it is deemed suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**).	YELLOW
	• A system exceeds the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login against an EACMS or BCS and locks out a system account and the Registered Entity confirmed the system account's password had changed but the accessing application/service had not yet been updated to use the new password.	GREEN	• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and failed login attempts. (**Determination of an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**).	ORANGE
			• Unknown individual attempts to login to a known default account on an EACMS or BCS, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and successfully gains unauthorized access to an EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**).	RED

Figure 9 Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

Example of Sample Criteria to Evaluate and Define Attempts to Compromise

An entity may establish criteria to evaluate and define attempts to compromise based on their existing capabilities and facilities associated with the other CIP Standards.

The sample criteria listed below are examples and are not intended to be exhaustive.

CIP-005 R1.5:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Detected known malicious or suspected malicious communications for both inbound and outbound communications.

CIP-005 R2.1:

Require multi-factor authentication for all Interactive Remote Access sessions.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Repeated attempts to authenticate using multi-factor authentication

CIP-007 R4.1:

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;
4.1.2. Detected failed access attempts and failed login attempts;
4.1.3. Detected malicious code.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Successful login attempts outside of normal business hours
- Successful login attempts from unexpected personnel such as those who are on vacation or medical leave
- Detected failed access attempts from unexpected network sources
- Detected failed login attempts to default accounts
- Detected failed login attempts from authorized personnel accounts exceeding X per day
- Detected failed login attempts from authorized personnel accounts where the account owner was not the source
- Detected malicious code on applicable systems

CIP-007 R5.7:

Where technically feasible, either:

- *Limit the number of unsuccessful authentication attempts; or*
- *Generate alerts after a threshold of unsuccessful authentication attempts.*

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Account locked due to limit of unsuccessful authentication attempts exceeded more than X times per day
- Threshold of unsuccessful authentication attempts exceeds more than X every Y minutes

CIP-010 R2.1:

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

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Detected unauthorized changes to the baseline configuration

An entity may establish additional criteria to evaluate and define attempts to compromise based on their infrastructure configuration:

Sample criteria:
Where investigation by entity determines that the specific activity, while malicious or/and suspicious:

- Attempt to compromise was not intended to target the “Applicable Systems”

Other Considerations

Protected Cyber Assets

A Protected Cyber Asset (PCA) is defined as:

> *One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.*[6]

It should be noted that PCAs are not one of the Applicable Systems and as such cyber incidents solely involving PCAs are not Cyber Security Incidents and are not reportable. Entities are encouraged to voluntarily report cyber incidents involving PCAs.

PCAs do reside within the ESP and as a result, some cyber incidents may be initiated on PCAs and later escalate into Cyber Security Incidents involving a BCS, the ESP or an EACMS.

Some examples are as follows:

1. A PCA is compromised or there was an attempt to compromise a PCA locally via removable media.

   This is not a Cyber Security Incident and is not reportable.

2. A PCA is compromised or there was an attempt to compromise a PCA from a source external to the ESP using an existing firewall rule.

   The compromise or attempt to compromise the ESP must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident, a Reportable Cyber Security Incident or an attempt to compromise.

3. A PCA is compromised or there was an attempt to compromise a PCA via an EACMS that has been compromised.

   The compromise of the EACMS must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident or a Reportable Cyber Security Incident.

4. A PCA is compromised and is also subsequently used as a pivot point to compromise or attempt to compromise a BCS.

   The compromise or attempt to compromise of the BCS must be evaluated against the entity's classification process (R1.2) to determine if this is a Cyber Security Incident, a Reportable Cyber Security Incident or an attempt to compromise.

[6] NERC Glossary of Terms https://www.nerc.com/files/glossary_of_terms.pdf

Requirement R1

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].*

1.1. One or more processes to identify, classify, and respond to Cyber Security Incidents.

1.2. One or more processes:

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 Reportable Cyber Security Incident 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. Provide notification per Requirement R4.

1.3. The roles and responsibilities of Cyber Security Incident response groups or individuals.

1.4. Incident handling procedures for Cyber Security Incidents.

Applicable Systems for the four collective Parts in Requirement R1 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R1

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

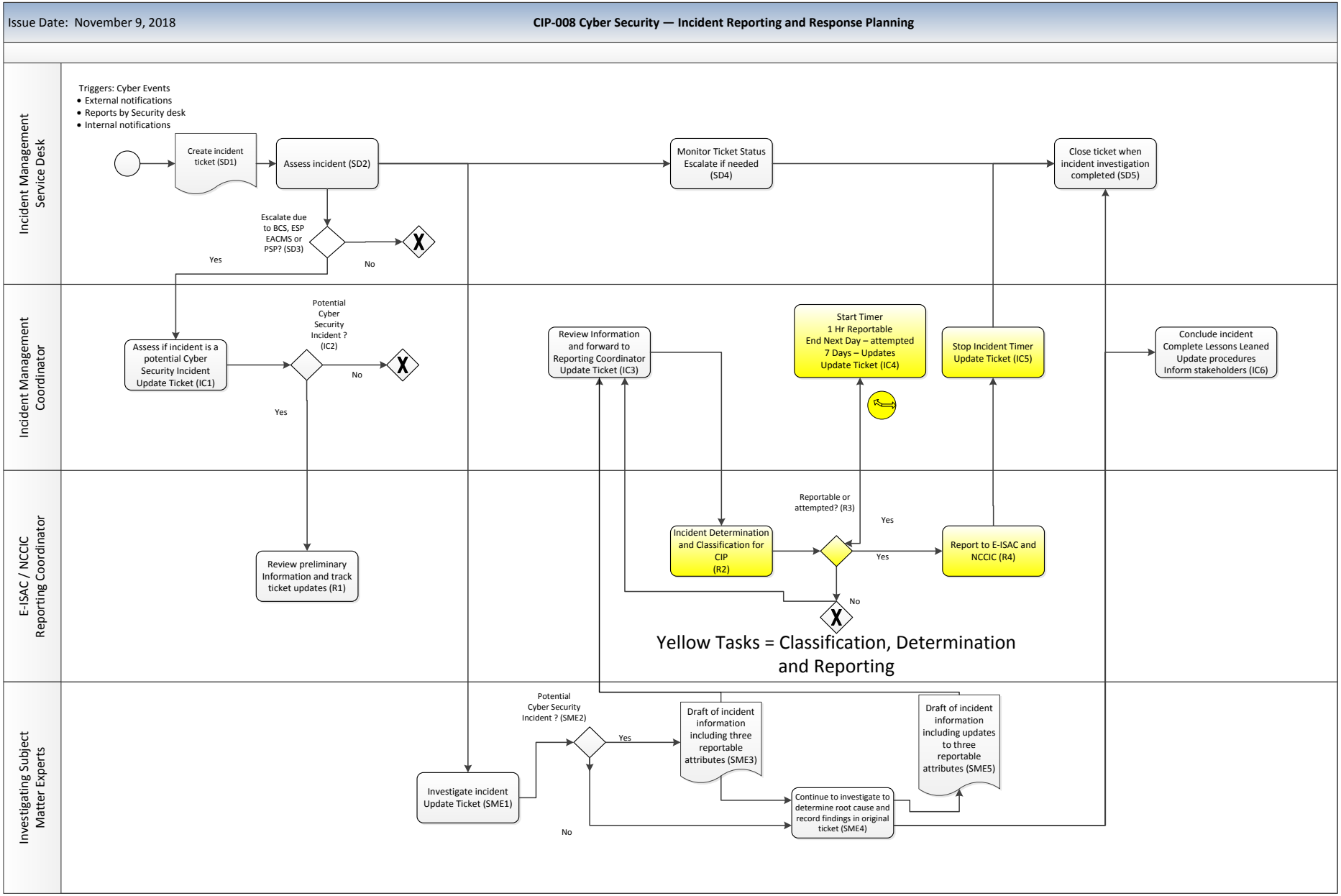


Figure 10 Sample Process to Identify, Classify and Respond to Cyber Security Incidents

Supporting Narrative Description of Sample Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

1. The Incident Management Service Desk identifies that a cyber event that requires investigation has occurred.
2. Incident Management Service Desk creates an incident ticket to log the suspected cyber incident (SD1).
3. Incident Management Service Desk performs initial assessment of the suspected cyber incident and performs any initial triage or service restoration as needed (SD2).
4. If the suspected cyber incident involves BES Cyber Systems (BCS), Electronic Access Control or Monitoring Systems (EACMS), Electronic Security Perimeter (ESP) or Physical Security Perimeters (PSP), the Incident Management Service Desk will escalate the incident to an Incident Management Coordinator whom will act as the coordinator until the incident is closed (SD3)
5. The Incident Management Coordinator performs a secondary initial assessment to determine if the incident has the potential to be a Cyber Security Incident, a Reportable Cyber Security Incident, or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

   They update the incident ticket, assigning the appropriate Investigating Subject Matter Experts (IC1).
6. If the Incident Management Coordinator determines that the incident has the potential to be reportable, the E-ISAC/ NCCIC Reporting Coordinator is alerted and copied on the information contained in the incident ticket. The E-ISAC/ NCCIC Reporting Coordinator continues to monitor the updates to the incident ticket (IC2).
7. The Incident Management Service Desk ensures the assigned Investigating SMEs are notified, and the incident ticket information is updated (SD2, SD4).
8. The assigned SMEs investigate the incident ticket updating with the Incident Management Coordinator as appropriate (SME1). The Incident Management Coordinator will monitor the progress of the investigation and assign additional SMEs or escalate as needed.
9. If initial investigation by SMEs finds that the incident may be a Cyber Security Incident and has the potential to be reportable (SME2), the SMEs will inform the Incident Management Coordinator and forward the known information including the required three attributes (SME3). Attributes which are unknown at the current time will be reported as "unknown".
10. The SMEs will continue their investigation to determine the root cause of the incident, performing triage or service restoration as needed, continue to investigate the three required attributes and update incident ticket information (SME4).
11. If the incident is found to be potentially reportable, the Incident Management Coordinator reviews the information, adds any details collected by other investigating SMEs and resolves any missing information as needed. The information is forwarded to the E-ISAC/ NCCIC Reporting Coordinator (IC3).
12. The E-ISAC/ NCCIC Reporting Coordinator reviews the information received, performs classification of the incident (R2). They determine if the incident is a Cyber Security Incident and determine if it is either a Reportable Cyber Security Incident or Cyber Security Incident that attempted to compromise

a system identified in the "Applicable Systems" column for the Part. The information to be reported is finalized (R3).

13. Upon determination that the incident is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a clock timer set to the appropriate time frame (IC4) and performs the required notification including the three required attributes. The incident ticket is updated with the incident classification and determination time for compliance evidence purposes:
    - Within 1 hour for initial notification of Reportable Cyber Security Incident,
    - By end of the next day for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, and
    - Within 7 calendar days of determination of new or changed attribute information required in Part 4.1, if any.

14. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator when notification is completed and time that the notifications occurred at. The Incident Management Coordinator will stop the appropriate timer and updates the incident ticket with the appropriate information for compliance evidence purposes (IC5).
15. If Incident Management Coordinator that has not received confirmation of notification, they may escalate, as needed, prior to expiry of the applicable timer. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4).
16. During the continued investigation of the incident (SME4), the SMEs may find that an update of any of the three required attributes is potentially required. The SMEs will inform the Incident Management Coordinator and forward a draft of the updated information (SME5)
17. The Incident Management Coordinator reviews the draft update information including adding other details, and then informs E-ISAC/ NCCIC Reporting Coordinator, forwarding the potential update information (IC3).
18. The E-ISAC/ NCCIC Reporting Coordinator reviews the potential updated information and determine if the update to any of the three required attributes is reportable (R3).
19. Upon determination that the update is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a timer set to the appropriate time frame (i.e. 7 calendar days). The incident ticket is updated with the determination time for compliance evidence purposes (IC4).
20. The E-ISAC/ NCCIC Reporting Coordinator updates both E-ISAC and NCCIC with the information associated with any of the three required attributes (R4).
21. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator that the update to E-ISAC and NCCIC is completed and times that the updates occurred at. The Incident Management Coordinator will stop the appropriate timer and update the incident ticket with the appropriate information for compliance purposes (IC5).

22. If the Incident Management Coordinator has not received confirmation that the update is completed, prior to the expiration of the timer, they may escalate as needed. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4).
23. Upon closure of the incident, the Incident Management Coordinator will ensure that the last reportable update to the three required attributes accurately reflects the closure information. If a further update of the three required attributes is required, the Incident Management Coordinator will inform the appropriate Subject Matter Expert to initiate an update (SME5).
24. The Incident Management Coordinator informs the Incident Management Service Desk that the incident ticket may be closed (SD5).
25. The Incident Management Coordinator will initiate a "Lessons Leaned" session and update to the Cyber Incident Reporting and Response Plan and any other documentation, procedures, etc. within 90 days (IC6). They will inform all stakeholders of any updates to the Cyber Incident Reporting and Response Plan and any other applicable documentation.

Roles and Responsibilities (R1.3)

In the example process, the defined Roles and Responsibilities are as follows, but can be tailored by any entity to align with their unique organization:

- Incident Management Service Desk is responsible for initial activities, incident ticketing and incident logging:
    - Initial identification, categorization and prioritization,
    - Initial diagnosis and triage/service restoration,
    - Initial assignment of incident tickets to Investigating Subject Matter Experts (SMEs)
    - Initial escalation to an Incident Management Coordinator upon assessment (if needed)
    - Monitoring incident ticket status and initiating further escalation (if needed)
    - Incident ticket resolution and closure
    - General incident status communication with the user community

- Incident Management Coordinator is responsible for the over-all coordination of activities related to an assigned incident:
    - Detailed assignment of tasks to Investigating SMEs
    - Ensure that all assigned activities are being performed in a timely manner
    - Ensuring regulatory reporting time limits are met and initiating escalation if needed
    - Communicating incident status with major affected stakeholders
    - Coordinating with the Incident Management Service Desk to update incident tickets with status and the logging of required details and assisting them to perform general incident status communications with the user community

- Coordinating with the E-ISAC/NCCIC Reporting Coordinator for cyber incidents with the potential of being Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Assisting the E-ISAC/NCCIC Reporting Coordinator with information to aid in the classification of the cyber incident.
- Escalation as needed according to the priority and severity of the issue
- Coordination of service restoration and incident closure
- Coordination of incident review following closure of incidents, identification of potential problems and documenting the "Lessons Learned"
- Initiating update of processes or procedures as needed and communicating the updates to stakeholders

- E-ISAC/ NCCIC Reporting Coordinator is responsible for the coordination of regulatory reporting activities such as those related to E-ISAC and NCCIC:
  - Review of completeness incident information for classification and reporting purposes
  - Incident classification for reporting purposes
  - Determination if this incident is a Cyber Security Incident, Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part
  - Completeness of the required three attributes to be reported
  - Notification to E-ISAC and NCCIC and submission of the three required attributes
  - Coordinating with Incident Management Coordinator to ensure timing is in accordance with regulatory requirements and that incident logging is complete for compliance evidence purposes

- Investigating Subject Matter Experts are responsible for detailed technical tasks related to the investigation of the incident and performing the needed recovery actions:
  - Perform investigation tasks related to the incident as assigned by the Incident Management Coordinator to determine the root cause of the incident
  - Perform service restoration tasks related to the incident as assigned
  - Update incident ticket and ensure all required details are logged
  - Obtaining information on the three required attributes for both initial notification and updates
  - After incident closure, participate in "Lessons Learned" sessions and update procedures as needed

Incident handling procedures for Cyber Security Incidents (R1.4)

Each of the defined roles in the example process may have specific procedures covering various aspects of their tasks being accomplished within the process. The sample process documents "what" the overall required steps are whereas the procedures document "how" each step is carried out:

- Incident Management Service Desk Procedures:
    - Procedures of when to classify cyber events as possible cyber incidents
    - Procedures to determine if BCS, PSP, ESP or EACMS are involved and decision criteria of when to escalate to an Incident Management Coordinator.
    - Procedures for initial diagnosis, triage and service restoration
    - Procedures for incident ticketing, assignment, escalation and closure

- Incident Management Coordinator Procedures:
    - Procedures for finding if cyber events or incidents could be possible Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. These potential incidents require notification to the E-ISAC/ NCCIC Coordinator
    - Procedures for the assignment and tracking of tasks to Investigating SMEs
    - Procedures associated with regulatory reporting time limits
    - Procedures for incident review, documentation of lessons learned, tracking of completion of documentation update status
- E-ISAC/ NCCIC Reporting Coordinator Procedures:
    - Procedures on how to use the Entity's own classification and reporting schema to classify cyber incidents and determine Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part
    - Procedures on the review of information to be used for reporting the three required attributes to be included for E-ISAC or NCCIC notification including the handling of any BES Cyber System Information
    - Procedures for the notification of updates to E-ISAC and NCCIC including the submission of the three required attributes
- Investigating Subject Matter Experts Procedures:
    - Procedures for the classification of cyber incidents to possible Cyber Security Incidents, possible Reportable Cyber Security Incidents or possible Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part and the required information needed to be obtained.
    - Procedures for troubleshooting tasks to determine root cause of an incident

- Procedures for service restoration tasks after an incident
- Procedures for triggering the forensic preservation of the incident
- Procedures on when updates are necessary to information on the required attributes associated with a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for the Part

Requirement R2

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]*

2.1. 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.

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.

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.

Applicable Systems for the three collective Parts in Requirement R2 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R2

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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, multi-discipline 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. 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.

[7] 2009, Department of Homeland Security, Developing an Industrial Control Systems Cybersecurity Incident Response Capability, page 13.

Requirement R3

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].*

3.1. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:

3.1.1. Document any lessons learned or document the absence of any lessons learned;

3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and

3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

3.2. No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:

3.2.1. Update the Cyber Security Incident response plan(s); and

3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.

Applicable Systems for the two collective Parts in Requirement R3 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

General Considerations for R3

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

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.

This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

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.

Requirement R4

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].*

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

Applicable Systems for the three collective Parts in Requirement R4 are the same, those being high impact BES Cyber Systems and their associated EACMS as well as medium impact BES Cyber Systems and their associated EACMS.

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"

NCCIC Reporting

NCCIC reporting guidelines for reporting events related to Industrial Control Systems can be found here:

https://ics-cert.us-cert.gov/Report-Incident
https://www.us-cert.gov/incident-notification-guidelines

NCCIC prefers the reporting of 10 attributes, although they will accept any information that is shared. A potential mapping between the NCCIC preferred attributes and the attributes required to comply with CIP-008-6 standard could be represented are as follows:

CIP-008-6 Reporting	NCCIC Reporting	Comment
Functional Impact	Identify the current level of impact on agency functions or services (Functional Impact).	
Functional Impact	Identify the type of information lost, compromised, or corrupted (Information Impact).	
Functional Impact	Identify when the activity was first detected.	
Level of Intrusion	Estimate the scope of time and resources needed to recover from the incident (Recoverability).	
Level of Intrusion	Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident	
Level of Intrusion	Identify the number of systems, records, and users impacted.	
Level of Intrusion	Identify the network location of the observed activity.	
Level of Intrusion	Provide any mitigation activities undertaken in response to the incident.	
Attack Vector	Identify the attack vector(s) that led to the incident.	
Name and Phone	Identify point of contact information for additional follow-up.	

Figure 11 NCCIC Reporting Attributes

Example of a Reporting Form

Entities may wish to create an internal standard form to be used to report Reportable Cyber Security Incidents and Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The advantages of using a standard internal form are:

- A standard internal format for the communications of cyber incident information between the various internal roles with respect to obligations of CIP-008-6, Requirement R4
- A standard written record of the notification of the minimum 3 attributes having been reported to E-ISAC and NCCIC in accordance with CIP-008-6, Requirement R4 which can be easily stored, sorted and retrieved for compliance purposes

An example of an internal standard form is shown. The instructions on how to complete this form are included after it.

CIP-008-6 Requirement R4

Cyber Security Incident Reporting Form

This form may be used to report Reportable Cyber Security Incidents and Cyber Security Incidents that were an attempt to compromise a system listed in the "Applicable Systems" column for the Part.

Contact Information

Name: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

Click or tap here to enter text.

Instructions for Example of a Reporting Form

These are instructions on one way to complete the optional form.

CIP-008-6
Cyber Security Incident Reporting Form Instructions

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
Contact Information	**Name**	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident. This field could also be used to identify the company name of the Registered Entity.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	**Reportable Cyber Security Incident**	Check this box if report includes information for a Reportable Cyber Security Incident.
	Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Check this box if report includes information for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if report is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if report is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.3.
Required Attribute Information (Attack Vector fields)	**Attack Vector**	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
	Attack Vector Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber System classification level.*
	Level of Intrusion Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If report is being used to provide an update, select the 'Update' checkbox.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-008-6 – Cyber Security — Incident Reporting and Response Planning

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

*CIP-008-6 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-003-8 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
P1.1			
P1.2			
P1.3			
P1.4			
R2			
P2.1			
P2.2			
P2.3			
R3			
P3.1			
P3.2			
R4			
P4.1			
P4.2			
P4.3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

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].*

M1. 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*.

R1 Part 1.1

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to identify, classify, and respond to Cyber Security Incidents.

Auditor Notes:

R1 Part 1.2

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes: 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 Reportable Cyber Security Incident; 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.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R1, Part 1.2
This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes that include criteria to evaluate and define attempts to compromise.
	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; 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.
	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to provide notification per Requirement R4.

Note to Auditor:
If the Responsible Entity is prohibited by law from reporting to the E-ISAC, then the process need not include a provision for reporting to the E-ISAC. If this provision is invoked, the audit team should verify that the Responsible Entity is prohibited by law from reporting to the E-ISAC.

If the Responsible Entity is within U.S. jurisdiction, but is prohibited by law from reporting to the NCCIC, then the process need not include a provision for reporting to the NCCIC. If this provision is invoked, the audit team should verify that the Responsible Entity is prohibited by law from reporting to the NCCIC.

Auditor Notes:

R1 Part 1.3

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which define the roles and responsibilities of Cyber Security Incident response groups or individuals.

Auditor Notes:

R1 Part 1.4

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include incident handling procedures for Cyber Security Incidents.

Auditor Notes:

R2 Supporting Evidence and Documentation

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].*

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.*

R2 Part 2.1

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has tested each Cyber Security Incident response plan 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.

Auditor Notes:

R2 Part 2.2

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6 R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity used the Cyber Security Incident response plan(s) reviewed under Requirement R1 when responding to a Reportable Cyber Security Incident, when responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or when performing an exercise of a Reportable Cyber Security Incident.
	Verify the Responsible Entity has documented deviations from the plan(s), if any, taken during the response to the Reportable Cyber Security Incident, to the Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or during the performance of an exercise of a Reportable Cyber Security Incident.
Note to Auditor: The practice of incident response requires the ability to be flexible when responding to Cyber Security Incidents. This is acknowledged by this Part's provision for documenting deviations from the Responsible Entity's incident response plan. The auditor should note that, while deviations from the incident response plan are permissible, deviations from the language of the Requirement (testing of the plan at least once every 15 calendar months, notification to the E-ISAC and NCCIC of applicable incidents, etc.), are not permissible.	

Auditor Notes:

R2 Part 2.3

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has retained 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.

Auditor Notes:

R3 Supporting Evidence and Documentation

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].*

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.*

R3 Part 3.1

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, the Responsible Entity has: 1. Documented any lessons learned or documented the absence of any lessons learned; 2. updated the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3. notified each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

Auditor Notes:

R3 Part 3.2

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, the Responsible Entity has: 1. Updated the Cyber Security Incident response plan(s); and 2. notified each person or group with a defined role in the Cyber Security Incident response plan of the updates.

Auditor Notes:

R4 Supporting Evidence and Documentation

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].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*.

R4 Part 4.1

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the initial notifications and updates included, to the extent known at the time: 1. The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted.

Auditor Notes:

R4 Part 4.2

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	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.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	For each Reportable Cyber Security Incident as identified pursuant to the process(es) specified in Requirement R1, Part 1.2, verify that the initial notification was submitted to each applicable agency within one hour after the determination of a Reportable Cyber Security Incident.
	For each Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, as identified pursuant to the process specified in Requirement R1, Part 1.2, verify that the initial notification was submitted to each applicable agency by the end of the next calendar day after a determination of a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part.

Auditor Notes:

R4 Part 4.3

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-6, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	For each Reportable Cyber Security Incident and each Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, verify updates, if any, were provided within 7 calendar days of determination of new or changed attribute information.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-008-6 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 706
See FERC Order 791
See FERC Order 848

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises, or attempts to compromise, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts, or attempts to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident

A Cyber Security Incident that 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.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
0	10/12/2018		New Document, based on CIP-008-5 RSAW
1	10/12/2018	RSAW Task Force	Revisions for CIP-008-6: • Updated version number • Minor text corrections • Added EACMS to applicability for all Parts • Modified wording for Parts 1.2, 2.2, and 2.3 • Added new R4 • Added new and revised Glossary terms
2	11/19/2018	RSAW Task Force	Revised for Draft 2
3	12/11/2018	SDT	Removed Item 1 under the 2.2 CAA as it is not needed. Revised 2.2 Note to Auditor. Minor text corrections.
4	1/11/2019	RSAW Task Force	Revised for Draft 3 ("Final" draft)
5	1/17/2019	RSAW Task Force	Revised for final version as posted

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Final Ballot Open through January 22, 2019

Now Available

An **8-day** final ballot for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** is open **Tuesday, January 15, 2019** through **8 p.m. Eastern, Tuesday, January 22, 2019.**

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pools associated with this project can log in and submit their vote here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 FN 3 ST
Voting Start Date: 1/15/2019 12:06:56 PM
Voting End Date: 1/22/2019 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 312
Total Ballot Pool: 324
Quorum: 96.3
Quorum Established Date: 1/15/2019 4:48:55 PM
Weighted Segment Value: 77.89

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	90	1	66	0.786	18	0.214	0	2	4
Segment: 2	7	0.7	3	0.3	4	0.4	0	0	0
Segment: 3	72	1	54	0.831	11	0.169	0	3	4
Segment: 4	18	1	14	0.824	3	0.176	0	0	1
Segment: 5	74	1	55	0.809	13	0.191	0	5	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	53	1	38	0.792	10	0.208	0	3	2
Segment: 7	1	0.1	0	0	1	0.1	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	8	0.7	7	0.7	0	0	0	1	0
Totals:	324	6.6	238	5.141	60	1.459	0	14	12

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		None	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Brandon McCormick	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Cleco Corporation	John Lindsey	Louis Guidry	Affirmative	N/A
1	CMS Energy - Consumers Energy Company	Donald Lynd		Negative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		Negative	N/A
1	Dairyland Power Cooperative	Renee Leidel		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Brandon McCormick	Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Negative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A
1	JEA	Ted Hobson		Negative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Negative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	N/A
1	Lower Colorado River Authority	Matthew Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	N/A
1	Portland General Electric Co.	Nathaniel Clague		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Negative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Chris Wagner		Negative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Negative	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	N/A
1	Westar Energy	Allen Klassen	Douglas Webb	Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		Negative	N/A
2	Midcontinent ISO, Inc.	David Zwergel		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Leanna Lamatrice		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	N/A
3	Black Hills Corporation	Eric Egge		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Clark Public Utilities	Jack Stamper		Abstain	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Affirmative	N/A
3	Gainesville Regional Utilities	Darko Kovac	Brandon McCormick	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski	Oshani Pathirane	Affirmative	N/A
3	Intermountain REA	David Maier		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	Brandon McCormick	Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Joseph Bencomo		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		Negative	N/A
3	Seattle City Light	Tuan Tran		Negative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Negative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bryan Taggart	Douglas Webb	Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	N/A
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Richard Comeaux		Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		Affirmative	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Affirmative	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	First Energy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza		Negative	N/A
5	JEA	John Babik		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NaturEner USA, LLC	Eric Smith		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Shivaz Chopra		Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Abstain	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Mark McDonald		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Richard Schlottmann		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	N/A
5	Vistra Energy	Dan Roethemeyer		Abstain	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Derek Brown	Douglas Webb	Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Negative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Luminant - Luminant Energy	Kris Butler		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Renee Knarreborg	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	N/A
6	New York Power Authority	Thomas Savin		Negative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Negative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Santee Cooper	Michael Brown		Negative	N/A
6	SCANA - South Carolina Electric and Gas Co.	John Folsom		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Negative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Negative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Grant Wilkerson	Douglas Webb	Affirmative	N/A
6	Western Area Power Administration	Charles Faust		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Luminant Mining Company LLC	Amanda Frazier		Negative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 324 of 324 entries

Exhibit I

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

	Name	Entity
Chair	Dave Rosenthal	MISO
Vice Chair	Kristine Martz	Exelon
Members	Katherine Anagnost	Minnkota Power
	Steve Brain	Dominion Energy
	John Breckenridge	Kansas City Power & Light Co; Westar Energy, Evergy companies
	Norm Dang	Independent Electricity System Operator of Ontario
	John Gasstrom	Georgia System Operations Corporation
	Tony Hall	LG&E and KU Energy
	Ian King	Xcel Energy
	Sharon Koller	American Transmisison Company, LLC
	Jennifer Korenblatt	PJM Interconnection
	Tina Weyand	EDP Renewables
PMOS Liaisons	Colby Bellville	Duke Energy
	Amy Casuscelli	Xcel Energy
NERC Staff	Alison Oswald – Senior Standards Developer	North American Electric Reliability Corporation
	Marisa Hecht – Counsel	North American Electric Reliability Corporation