NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Incident Report

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

January 2019

RELIABILITY | ACCOUNTABILITY



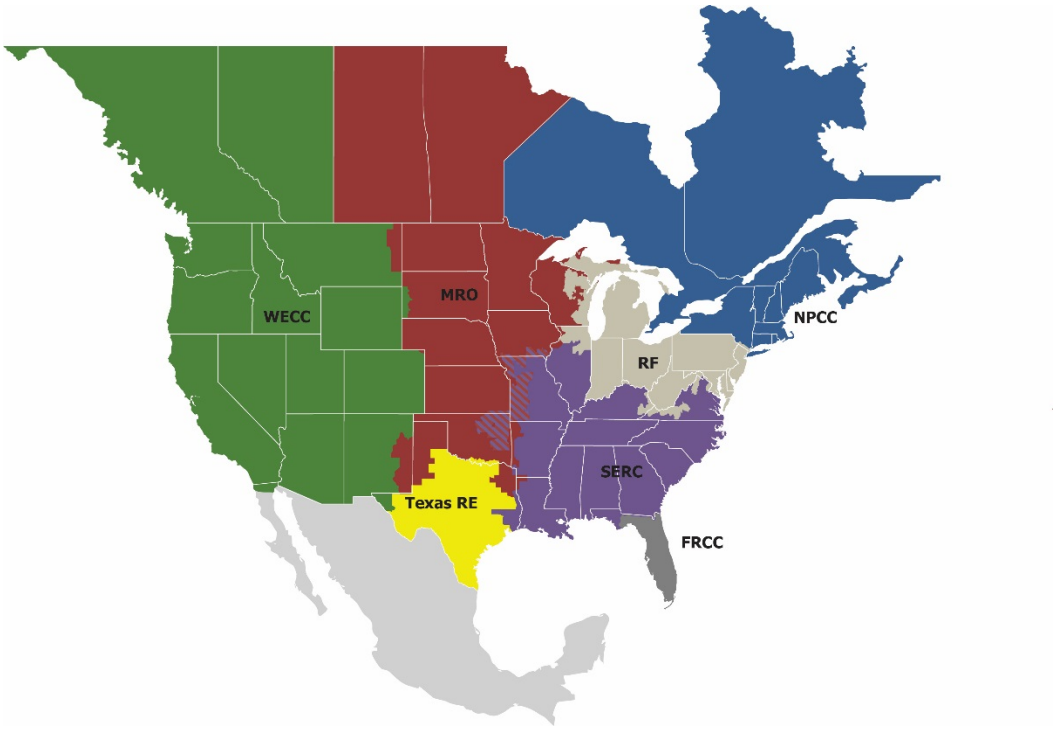

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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*.

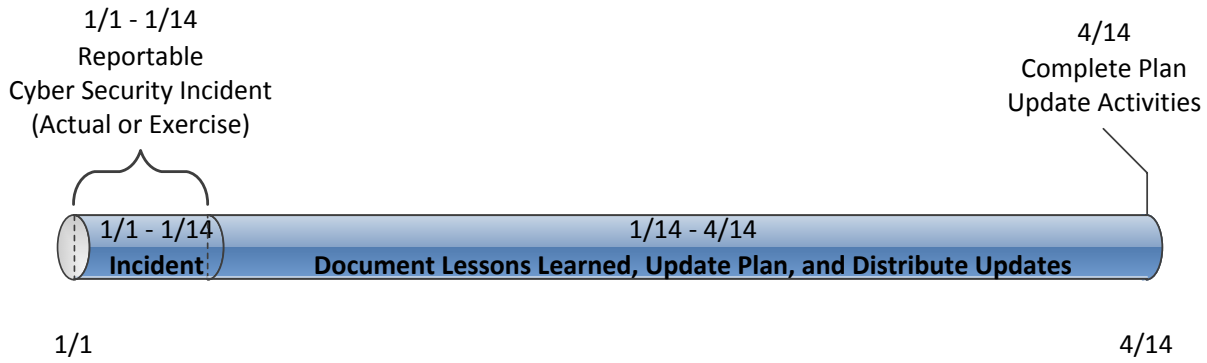
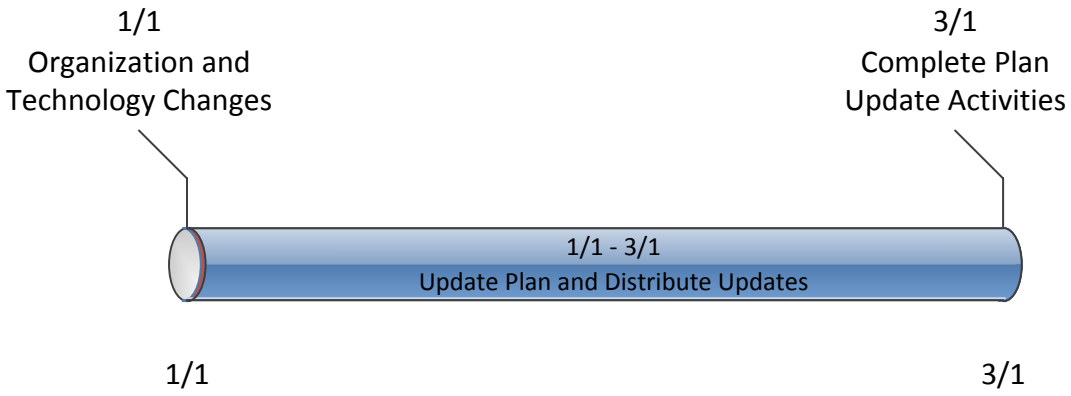


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

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