Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, 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. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

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	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

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

2. Number: CIP-008-5

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 Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- 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.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

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

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

4.2.4.3 In nuclear plants, 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.

5. 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 a common subject matter.

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. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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 they feel 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.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. 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 applicability 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

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. Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements. 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: The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 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 items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Processes to identify, classify, and respond to Cyber Security Incidents.	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.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident.	Evidence may include, but is 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.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *EOP-004-2 will address 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.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	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.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	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, post-incident analysis).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*	

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 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.

R2. Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 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 items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test the BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months between executions of the plan(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise; or • With a full operational exercise.	Evidence may include, but is 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.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the incident response plan under Requirement R1 when responding to or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan during the response to the incident or exercise.	Evidence may include, but is 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.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain relevant records related to Reportable Cyber Security Incidents.	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.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *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 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.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews.	Evidence may include, but is not limited to, dated documentation of a review of each Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months between reviews, and an updated Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Specified what the annual review entails.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after completion of the test or actual incident response.	Evidence may include, but is not limited to, dated documentation of lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within 30 calendar days after completion of the test or actual incident response.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.	Evidence may include, but is not limited to: • Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or • A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.

Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*	
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.	Evidence may include, but is not limited to, dated documentation reflecting changes made to the Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the Responsible Entity determined would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *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.*	

3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies activities required to maintain the plan.*	

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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- 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 duration specified above, whichever is longer.
- The Compliance Enforcement Authority 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

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			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 the Cyber Security Incident response plan(s), but	The Responsible Entity has not developed a Cyber Security Incident response plan 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 processes to identify Reportable Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the plan does not include internal groups or individuals or external organizations that should receive communication of the Cyber Security Incident. (1.5)	
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 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) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. OR The Responsible Entity does not use its Cyber Security Incident response plan during a test or when a Reportable Cyber Security Incident occurs. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 and less than 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 60 calendar days after the documentation required by 3.1. (3.2) OR	The Responsible Entity has not documented any lessons learned within 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes. OR The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The following guidelines are available to assist in addressing the required components of an 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 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 should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.

Requirement R2:

Requirement R2 ensures entities periodically test the 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. TTXs 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 3.2 and (2) organizational or technology changes from Part 3.4.

The documentation of lessons learned from Part 3.2 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 BES Reportable Cyber Security Incident without any documented lessons learned.

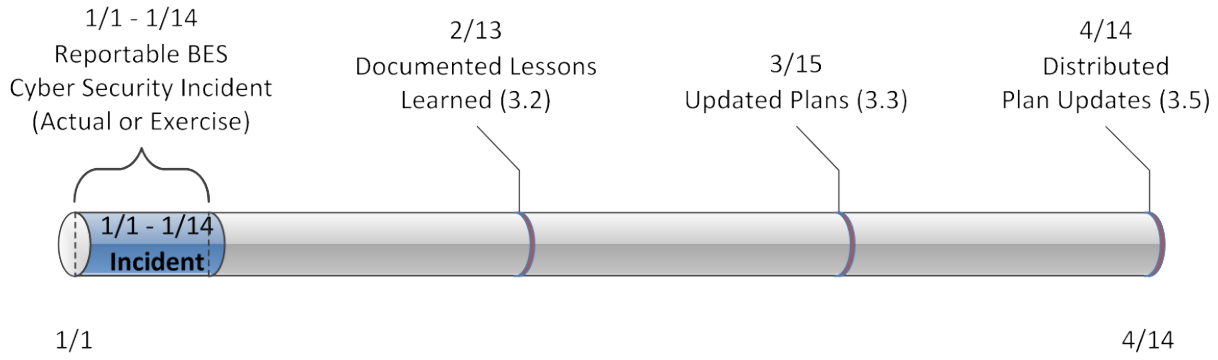

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.

Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.

The plan change requirement in Part 3.4 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.

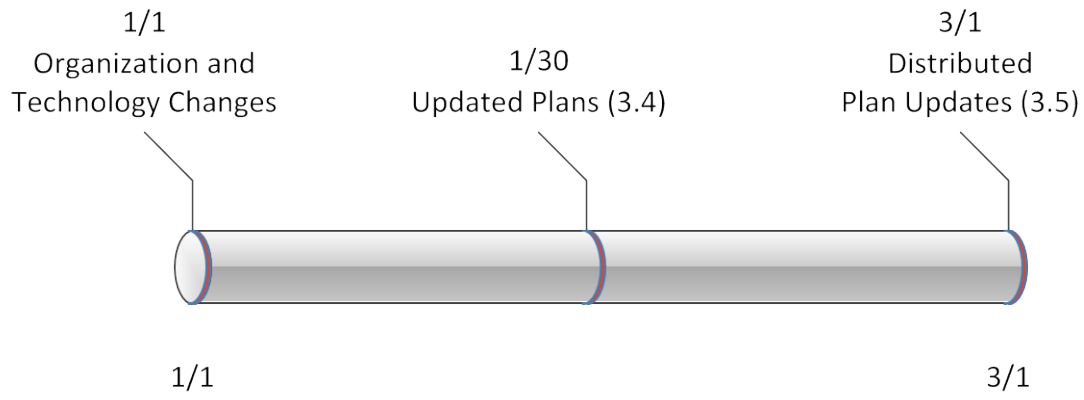

Figure 2: Timeline for Plan Changes in 3.4