

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: <ul style="list-style-type: none"> • EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>One or more processes:</p> <p>1.2.1 That include criteria to evaluate and define attempts to compromise;</p> <p>1.2.2 To determine if an identified Cyber Security Incident is:</p> <ul style="list-style-type: none"> 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 <p>1.2.3 To provide notification per Requirement R4.</p>	<p>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.</p>

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • EACMS 	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: <ul style="list-style-type: none"> • 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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.</p>	<p>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.</p>
2.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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.</p>	<p>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.</p>

- 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:</p> <p>3.1.1. Document any lessons learned or document the absence of any lessons learned;</p> <p>3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and</p> <p>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.</p>	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 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; Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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:</p> <p>3.2.1. Update the Cyber Security Incident response plan(s); and</p> <p>3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.</p>	<p>An example of evidence may include, but is not limited to:</p> <ol style="list-style-type: none"> Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and Evidence of plan update distribution including, but not limited to: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • EACMS Medium Impact BES Cyber Systems and their associated: <ul style="list-style-type: none"> • EACMS 	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: <ul style="list-style-type: none"> 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	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>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:</p> <ul style="list-style-type: none"> 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. 	<p>Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.</p>
4.3	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> EACMS 	<p>Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.</p>

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	<p>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)</p> <p>OR</p> <p>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)</p> <p>OR</p> <p>The Responsible Entity has developed a Cyber</p>	<p>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)</p> <p>OR</p> <p>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</p>

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
					<p>OR</p> <p>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)</p>	<p>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)</p>
R3	Operations Assessment	Lower	<p>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</p>	<p>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</p>	<p>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</p>	<p>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</p>

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) <ul style="list-style-type: none"> • 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) <ul style="list-style-type: none"> • 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
			<p>timelines pursuant to Part 4.2. (4.2)</p> <p>OR</p> <p>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)</p> <p>OR</p> <p>The Responsible Entity notified E-ISAC and NCCIC, or their</p>	<p>“Applicable Systems” column. (R4)</p>	<p>The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)</p>	

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	