A. Introduction

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

2. **Number:** CIP-008-7

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 Bulk Electric System (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 (RAS) where the RAS 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 RAS where the RAS 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-008-7:

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

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 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.

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

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

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

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-008-7 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-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are 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-008-7 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-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	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.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 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-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), 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-008-7 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-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

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:
   As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			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. (Part 2.2)	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. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify 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. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update 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. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column. (Requirement R4)	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Version	Date	Action	Change Tracking
7	TBD	Virtualization Modifications	
7	5/9/2024	Adopted by the NERC Board of Trustees	