

## A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-4
3. **Purpose:** Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.
4. **Applicability**
  - 4.1. Within the text of Standard CIP-008-4, “Responsible Entity” shall mean:
    - 4.1.1 Reliability Coordinator.
    - 4.1.2 Balancing Authority.
    - 4.1.3 Interchange Authority.
    - 4.1.4 Transmission Service Provider.
    - 4.1.5 Transmission Owner.
    - 4.1.6 Transmission Operator.
    - 4.1.7 Generator Owner.
    - 4.1.8 Generator Operator.
    - 4.1.9 Load Serving Entity.
    - 4.1.10 NERC.
    - 4.1.11 Regional Entity.
  - 4.2. The following are exempt from Standard CIP-008-4:
    - 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.
    - 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
    - 4.2.3 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
    - 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.
5. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

- R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
  - R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

- R1.2.** Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.
- R1.3.** Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
- R1.4.** Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
- R1.5.** Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
- R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.
- R2.** Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

#### **C. Measures**

- M1.** The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.
- M2.** The Responsible Entity shall make available all documentation as specified in Requirement R2.

#### **D. Compliance**

##### **1. Compliance Monitoring Process**

###### **1.1. Compliance Enforcement Authority**

###### **1.2. The RE shall serve as the CEA with the following exceptions:**

- 1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- 1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 1.2.3** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- 1.2.4** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

###### **1.3. Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information

**1.5.1** The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

**1.5.2** The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

## 2. Violation Severity Levels (To be developed later.)

### E. Regional Variances

None identified.

### Version History

Version	Date	Action	Change Tracking
2		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 NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)