A. Introduction

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

2. Number: CIP-008-1

3. Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

4. Applicability

4.1. Within the text of Standard CIP-008, "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 Reliability Organizations.

4.2. The following are exempt from Standard CIP-008:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or 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 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. 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 incident response teams, 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 ninety 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 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

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

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

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

2. Levels of Noncompliance

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking