A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 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-009-3, "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-009-4:

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. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

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 required by Standard CIP-009-4 from 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

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	MEDIUM	N/A	The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-4 R1.1 **or** R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-4 R1.1 **and** R1.2.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	MEDIUM	N/A	N/A	N/A	N/A
R2	LOWER	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
R3	LOWER	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R4	LOWER	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
R5	LOWER	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

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. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the 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)
4	4/19/12	FERC Order issued approving CIP-009-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
4	8/12/13	FERC Order issued granting an extension of time on CIP V4 Reliability Standards. This order extends the enforcement date from April 1, 2014 to October 1, 2014.	