Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~

~~8.~~3. ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy~~)November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012

BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this ~~implementation plan~~Implementation Plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their ~~implementation plan~~Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the ~~implementation plan~~Implementation Plan and standards for CIP-002-4 through CIP-009-4.

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.~~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.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber ~~Assets and~~ Systems

2. Number: CIP-009-5

~~**3. Purpose:** Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.~~

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

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 Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSUVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.24.2.3 where the**Generator Operator**

4.2.34.2.4 **Generator Owner**

4.2.44.2.5 **Interchange Coordinator**

4.2.5 Load Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.6 NERC

4.2.7 Regional Entity

4.2.84.2.6 **Reliability Coordinator**

4.2.94.2.7 **Transmission Operator**

4.2.104.2.8 **Transmission Owner**

4.3. Facilities:

4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ 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.

~~**4.3.3**~~**4.3.1 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~009~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~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.

~~**4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.**~~

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

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 ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence

example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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 ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and 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 subject matter. Examples in the ~~Standards~~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.~~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.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. 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 applicability column as described.

- ~~**All Responsible Entities –** Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~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.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity –** Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- ~~**Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These~~

~~hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

~~**Rationale for R1:** Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.~~

~~**Summary of Changes:**~~

~~Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.~~

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning~~]~~].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but ~~-~~is ~~-~~not limited to, one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** ~~*Reworded to address FERC Order 706 P694 and simplify the*~~*Minor wording*~~.~~ *changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders~~, including identification of the individuals, either by name or by title, responsible for recovery efforts~~.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders~~, including identification of the individuals responsible for recovery efforts.~~.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup~~,~~ and storage~~, and protection~~ of information required to ~~restore~~recover BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, ~~and protection~~ of information required to successfully ~~restore a~~recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirements**	**~~Part~~Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence ~~of the verification~~or logs confirming that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Preserve data, where technically feasible~~Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s~~) as required in Requirement R1. ~~).	Evidence may include, but is not limited to, procedures to preserve data~~,~~; such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, ~~paragraph~~Paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an ~~emergency~~Emergency and their responses to a particular ~~emergency~~Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for ~~emergencies~~Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, ~~emergency~~Emergency notifications, ~~system~~System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.~~28~~ Functional exercises allow staff to execute their roles and responsibilities as they would in an actual ~~emergency~~Emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: ~~Long Term~~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 items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Implement~~Test the recovery plan(s) referenced in Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between ~~executions~~tests of the plan: • ~~by~~By recovering from an actual incident~~, or~~; • ~~with~~With a paper drill or tabletop exercise~~,~~; or • ~~with a full~~With an operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with ~~a full~~an operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media ~~initially and~~ at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.	Evidence may include, but is not limited to, dated evidence of a test of ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC ~~Requirements (~~Order No. 706, Paragraphs 739~~,~~ and 748~~)~~ related to testing of backups.*	
2.3	High Impact BES Cyber Systems ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	Test each of the recovery plans referenced in Requirement R1~~, initially upon the effective date of the standard, and~~ at least once every ~~39~~36 calendar months ~~thereafter~~ through an operational exercise of the recovery plans in ~~a~~ an environment representative ~~environment that reflects~~of the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to~~:~~ Dated evidence of ~~an~~: • An operational exercise ~~initially upon~~prior to the effective date of the standard and at least once every ~~39~~36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual incident response which occurred within the ~~39~~36 calendar month timeframe that ~~implemented~~exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC ~~Requirement (~~Order No. 706, Paragraph 725~~)~~ to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: ~~Long-Term Planning~~]Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document~~Document any identified deficiencies or lessons learned~~.~~ associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.	Evidence may include, but is not limited to, dated ~~evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including~~ documentation of ~~any~~ identified deficiencies or lessons learned for each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the time frame for update.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.	Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.
Reference to prior version: *CIP-009, R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~**Reference to prior version:**~~ ~~*CIP-009-R1*~~Update recovery plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.	~~**Change Description and Justification:**~~ ~~*Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*~~ Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.
Reference to prior version: *CIP-009-R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).
Reference to prior version: *CIP-009-R3*		**Change Description and Justification:** *Added the timeframe for update.*	

~~CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication~~			
~~Part~~	~~Part~~	~~Part~~	~~Part~~
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.~~	~~Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).~~

Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.~~5~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Communicate all~~Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within ~~thirty~~30 calendar days of the update being completed.	Evidence of ~~communication~~ distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or anothera Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaintcompliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority 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

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long ~~Term~~ term Planning**	**Medium**	N/A	~~N/A.~~The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery ~~plans,~~plan(s), but the ~~plans~~plan(s) do not address ~~all~~two of the requirements included in ~~Items~~Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber ~~Assets and~~ Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems ~~that~~, but the plan(s) does not address the conditions for activation~~,~~ ~~including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to~~ in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service~~Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	~~**Long Term**~~**Operations Planning** **Real-time Operations**	**Lower**	~~N/A~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR	~~N/A~~The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible	The Responsible Entity has not tested the ~~information used in the~~ recovery ~~of BES Cyber Systems that is stored on backup media initially and at least once each calendar year~~plan(s) according to R2 Part 2.1 within 17 calendar months, not ~~to exceed~~	The Responsible Entity has ~~failed to conduct a~~ not tested the recovery plan ~~test initially upon the effective date~~(s) according to R2 Part 2.1 within 18 calendar months between tests of the ~~standard and at least once each calendar year~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	15exceeding 18 calendar months between tests. of the plan. (2.1) OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 yearsinformation used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not to exceedexceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part	thereafter, not plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to exceed 15R2 Part 2.2 within 19 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, that is an operational exercise in a representative environment to demonstrate readiness.~~. (2.3)	
R3	~~Long Term Planning~~**Operations Assessment**	**Lower**	~~N/A~~The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)	~~N/A~~The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1) OR The Responsible	The Responsible Entity has not ~~reviewed and~~ documented ~~the results of its~~any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery~~ within 30 calendar days of its execution.~~. (3.1)	The Responsible Entity has not ~~reviewed its recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced.~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3) OR The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)	OR The Responsible Entity has not updated ~~its~~the recovery plan(s) based on any documented ~~deficiencies or~~ lessons learned within ~~30~~60 calendar days after the documentation required by R3 Part 3.2. (3.2) OR The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar days of any of ~~its execution.~~the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to	~~OR~~ ~~The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel~~documented any lessons learned within ~~30~~60 calendar days of ~~completing the updates.~~each recovery plan test or actual incident recovery. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					execute the plan. (3.3)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS~~).~~)