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. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-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. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the 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.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-009-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of 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 (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the 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. 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 "Guidelines and Technical Basis" section of the Standard.

A. Introduction

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

2. Number: CIP-009-5

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~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~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~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~4.1.2 ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~:~~

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

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 ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~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 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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.

~~4.2.3~~4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3 Exemptions: The following are exempt from Standard CIP-~~002~~009-5:

~~4.2.4.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3 ~~In nuclear plants, the Systems~~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.

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

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*.

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

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~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 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 imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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 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.
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.

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 applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~**Applicability Columns in Tables:**~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems 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~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as 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 according to the CIP-002-5 identification and categorization processes.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high 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 (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES

Cyber System or medium impact BES Cyber System with External Routable Connectivity ~~in the applicability column~~.

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~~System functionality 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~~requirement parts 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~~requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	~~Evidence~~An example of 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:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Roles and responsibilities of responders.	~~Evidence~~An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	~~Evidence~~An example of evidence may include, but is not limited to, documentation of specific processes for the backup~~,~~ and storage~~,~~ of information required to ~~successfully~~ recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** ~~*Minor*~~*Addresses FERC Order Paragraph 739 and 748. The modified* wording ~~*changes; essentially unchanged*~~*was abstracted from Paragraph 744*.	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~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.~~One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated evidence or~~ logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	

1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems. and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Processes~~One or more processes to preserve data~~, except~~ for ~~CIP Exceptional Circumstances, for analysis or diagnosis of~~determining the cause of ~~any event~~a Cyber Security Incident that triggers activation of the recovery plan(s~~). ~~), per device capability. Data preservation should not impede or restrict recovery.	~~Evidence~~An example of evidence may include, but is not limited to, procedures to preserve data~~;~~, such as preserving a corrupted drive~~,~~ or 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 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 and their responses to a particular 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 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 notifications, 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. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual Emergency situation, but in a simulated manner.~~

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

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

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R2 – Recovery 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 ~~items~~requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Test each of the recovery ~~plan(s)~~plans referenced in Requirement R1 at least once ~~each calendar year, not to exceed~~every 15 calendar months between tests of the plan: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	~~Evidence~~An example of 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 an operational exercise) of the recovery plan at least once ~~each calendar year, not to exceed~~every 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.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Test a representative sample of information used ~~in the recovery of~~ to recover BES Cyber ~~Systems that is stored on backup media~~System functionality at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between tests,~~ to ensure that the information is useable and is compatible with current ~~system~~ configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated evidence of a~~operational logs or test ~~of information used in~~results with criteria for testing the ~~recovery of BES Cyber Systems that is stored on backup media when initially stored~~usability (e.g. sample tape load, browsing tape contents) and ~~at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible~~compatibility with current system configurations~~.~~ (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** ~~*Combined*~~*Specifies what to test and makes clear the test can be a representative sampling. These changes, along with* Requirement ~~*from CIP-009 R5 included requirement to test when initially stored. Addresses*~~*Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary*.	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	~~Evidence~~ Examples of evidence may include, but ~~is~~are not limited to ~~Dated evidence~~, dated documentation of: • An operational exercise ~~prior to the effective date of the standard and~~ at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual ~~incident~~recovery response ~~which~~that occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC 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~~improve 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~~ (s) following a test, and to ensure ~~that~~ the maintenance and distribution of the recovery ~~plans remain updated~~plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and ~~individuals are aware of the~~ (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates~~.~~ and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

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

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

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Document any identified deficiencies or lessons learned associated with each~~ After completion of a recovery plan test or actual ~~incident~~ recovery ~~within 30~~, and not to exceed 90 calendar days ~~after completion of~~ : 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the ~~test or recovery.~~ absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~Evidence~~An example of evidence may include, but is not limited to, ~~dated~~all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery ~~within 30 calendar days after completion of the test~~ or dated documentation stating there were no lessons learned; 2. Dated and revised recovery 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.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**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~~**Reference to prior version:** *CIP-009, R1 and R3*	~~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.~~**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates.This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*	~~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	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.~~3~~2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Update recovery plan(s) within 30 calendar days of any of~~ After a change to the ~~following changes~~roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~the plan or~~ the ability to execute the recovery plan, and not to exceed 60 calendar days: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan~~:~~ of the updates. ~~• Roles or responsibilities; or~~ ~~• Technology changes.~~	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated documentation reflecting~~all of the following: Dated and revised recovery plan with 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:~~ 1. ~~Roles~~roles or responsibilities~~;~~, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • ~~Technology changes.~~Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~Reference to prior version:~~ ~~*New Requirement*~~		**~~Change Description and Justification:~~** ~~*Ensures that recovery plans stay updated.*~~	
~~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~~	~~Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within 30 calendar days of the update being completed.~~	~~Evidence of 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*~~ *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to* any changes ~~*to recovery plans*~~*. The modifications make clear the specific changes that would require an update.*	

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~~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 ~~Compliance Enforcement Authority~~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 ~~data or~~ evidence ~~for~~of 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 mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA 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 Planning	Medium	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 plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	Operations Planning Real-time	Lower	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations		2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR 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)	not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible 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)	2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 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
R3	Operations Assessment	Lower	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)	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 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)	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery. (3.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 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	The Responsible Entity has not documented any lessons learned within 60 calendar days of 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
				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)	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)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

~~(SEE FAQs AND CIPC GUIDELINES AS A BASIS.)~~**Section 4 – Scope of Applicability of the CIP Cyber Security Standards**

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

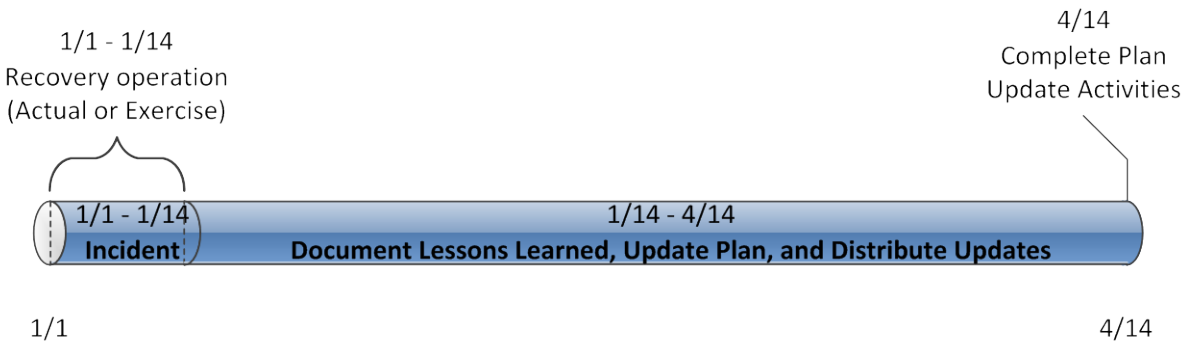
The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

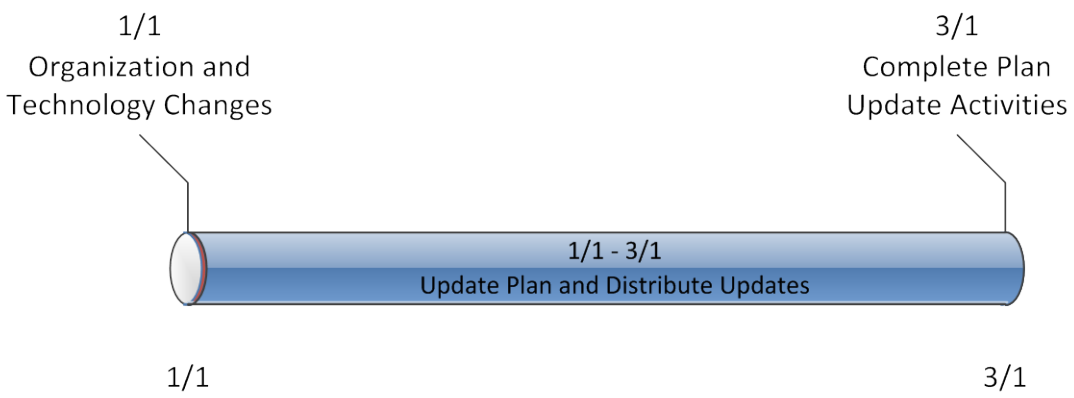
The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.



R1. **Figure 1: CIP-009-5 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.



R2. **Figure 2: Timeline for Plan Changes in 3.2**

When notifying individuals of response plan changes, entities should keep in mind that recovery plans are considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.