Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

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

2. **Number:** CIP-009-76

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 one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

        4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

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

            4.1.2.1.2 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. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

        4.1.2.3. 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.

        4.1.2.4. 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.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **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~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS 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.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-009-76:

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

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. 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.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-75.1 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan" ~~for CIP-009-76.~~

~~6.~~ ~~**Background:** Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~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 the requirement's common subject matter.~~

~~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 it believes 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 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.

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 "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. 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 "Applicable Systems" column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 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-002-5.1 identification and categorization processes.

Electronic Access Control or Monitoring Systems (EACMS) – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-76 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 requirement parts in *CIP-009-76 Table R1 – Recovery Plan Specifications*.

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**

1.2	High Impact ~~BES Cyber Systems~~BCS and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	Medium Impact ~~BES Cyber Systems~~BCS and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	SCI hosting High or Medium Impact BCS or their associated:
	
	   • PACS; or
	
	   • EACMS
		Roles and responsibilities of responders.	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.

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes for the backup and storage of information required to recover ~~BES Cyber System~~applicable system functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber System~~ applicable system functionality.

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS 1. ~~EACMS; and~~ 2. ~~PACS~~ Medium Impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. PACS; and 2. EACMS 1. ~~EACMS; and~~ 2. ~~PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009-76 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**

1.5	High Impact ~~BES Cyber Systems~~ BCS and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	Medium Impact ~~BES Cyber Systems~~ BCS and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	SCI hosting High or Medium Impact BCS or their associated:
	
	   • PACS; or
	
	   • EACMS
		One or more processes to preserve data, per ~~Cyber Asset~~ system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	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.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-76 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 requirement parts in *CIP-009-76 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**

2.1	High Impact ~~BES Cyber Systems~~BCS and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	Medium Impact B~~ES Cyber Systems~~BCS at Control Centers and their associated:
	
	   1. PACS; and
	
	   2. EACMS
	
	   ~~1. EACMS; and~~
	
	   ~~2. PACS~~
	
	SCI hosting High or Medium Impact BCS at Control Centers or their associated:
	
	   • PACS; or
	
	   • EACMS
		Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:
		
		• By recovering from an actual incident;
		
		• With a paper drill or tabletop exercise; or
		
		• With an operational exercise.
			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 every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. PACS; and 2. EACMS 1. ~~EACMS; and~~ 2. ~~PACS~~ Medium Impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. PACS; and 2. EACMS 1. ~~EACMS; and~~ 2. ~~PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	Test a representative sample of information used to recover ~~BES Cyber System~~ applicable system functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber System~~ applicable system functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-76 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~BCS SCI hosting High Impact ~~BES Cyber Systems~~BCS	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.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-76 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 requirement parts in *CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-76 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**

3.1	High Impact ~~BES Cyber Systems~~BCS and their associated:
	
	  1. PACS; and
	  2. EACMS
	  ~~1. EACMS; and~~
	  ~~2. PACS~~
	
	Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated:
	
	  1. PACS: and
	  2. EACMS
	  ~~1. EACMS; and~~
	  ~~2. PACS~~
	
	SCI hosting High or Medium Impact BCS at Control Centers or their associated:
	
	  • PACS; or
	  • EACMS
		No later than 90 calendar days after completion of a recovery plan test or actual recovery:
		
		3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;
		
		3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; 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.
			An example of evidence may include, but is not limited to, all of the following:
			
			1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery 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-009-76 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**

3.2	High Impact ~~BES Cyber Systems~~BCS and their associated:
	
	1. PACS; and
	2. EACMS
	1. ~~EACMS; and~~
	2. ~~PACS~~
	
	Medium Impact ~~BES Cyber Systems~~BSC at Control Centers and their associated:
	
	1. PACS; and
	2. EACMS
	1. ~~EACMS; and~~
	2. ~~PACS~~
	
	SCI hosting High or Medium Impact BCS at Control Centers or their associated:
	
	• PACS; or
	• EACMS
		No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:
		
		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.
			An example of evidence may include, but is not limited to, all of the following:
			
			1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and
			
			2. Evidence of plan update distribution including, but not limited to:
			
			  • Emails;
			  • USPS or other mail service;
			  • Electronic distribution system; or
			  • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. **Compliance Enforcement Authority:**

    As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

    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 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 evidence of each requirement in this standard for three calendar years.

    - 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 time specified above, whichever is longer.

    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

    1.4. ~~Compliance Monitoring and Assessment Processes:~~

    - ~~Compliance Audits~~

    - ~~Self-Certifications~~

    - ~~Spot Checking~~

    - ~~Compliance Investigations~~

    - ~~Self-Reporting~~

    - ~~Complaints~~

    1.5. ~~Additional Compliance Information:~~

    ~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 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 Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~BES Cyber Systems~~applicable systems. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R2.	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. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 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	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 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. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	tests. (Requirement R2 Part 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. (Requirement R2 Part 2.3)	months between tests. (Requirement R2 Part 2.3)	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. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2)	

R #	Violation Severity Levels (CIP-009-76)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			• Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan."

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	12/16/09	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.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Guidelines and Technical 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.

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-002-5.1'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
Installation files and media;
Current backup tapes and any additional documented configuration settings;
Documented build or restoration procedures; and
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.

1/1 - 1/14
Recovery operation
(Actual or Exercise)

4/14
Complete Plan
Update Activities

1/1 - 1/14	1/14 - 4/14
Incident	Document Lessons Learned, Update Plan, and Distribute Updates

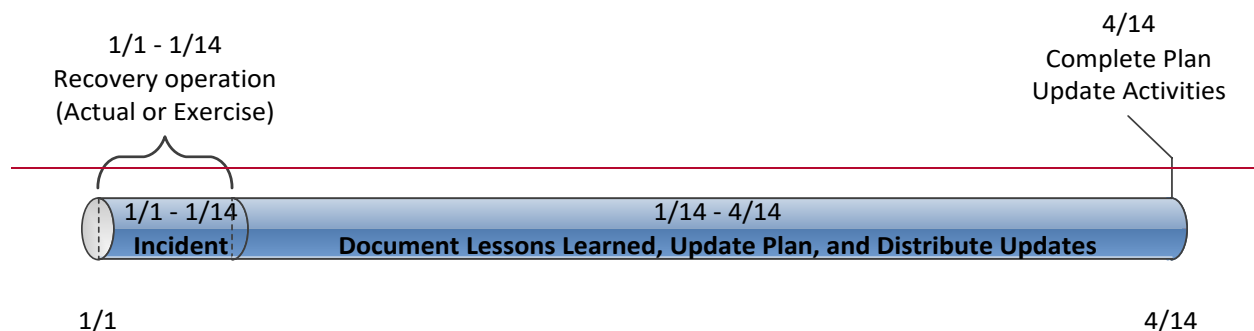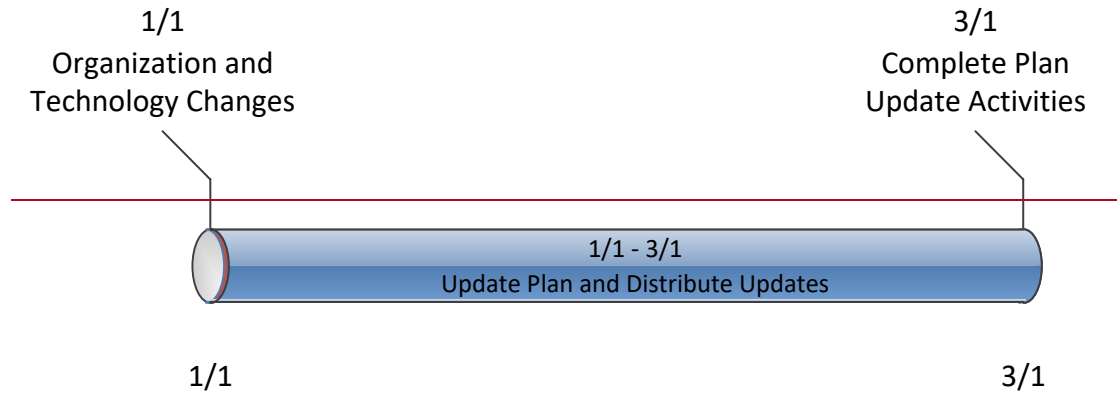1/1   4/14

Figure 1: CIP-009-6 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.

Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be 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.

Rationale:

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement 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 System functionality occurs.~~

~~Rationale for Requirement 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.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (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.~~