

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-009-7
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 Remedial Action Scheme (RAS) where the 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. Reliability Coordinator

4.1.6. Transmission Operator

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 RAS where the 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-009-7:

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

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

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-009-7 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-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BCS and their associated: <ol style="list-style-type: none"> 1. PACS; and 2. EACMS Medium Impact BCS and their associated: <ol style="list-style-type: none"> 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: <ul style="list-style-type: none"> • 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-009-7 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>Roles and responsibilities of responders.</p>	<p>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.</p>
1.3	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>One or more processes for the backup and storage of information required to recover applicable system functionality.</p>	<p>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 applicable system functionality.</p>

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.4	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.</p>	<p>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.</p>
1.5	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>One or more processes to preserve data, per 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.</p>	<p>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.</p>

- R2.** Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7 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-009-7 Table R2 – Recovery Plan Implementation and Testing*.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BCS and their associated: <ol style="list-style-type: none"> 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: <ol style="list-style-type: none"> 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: <ul style="list-style-type: none"> • PACS; or • EACMS 	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: <ul style="list-style-type: none"> • 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-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>Test a representative sample of information used to recover applicable system functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.</p> <p>An actual recovery that incorporates the information used to recover applicable system functionality substitutes for this test.</p>	<p>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).</p>
2.3	<p>High Impact BCS</p> <p>SCI hosting High Impact BCS</p>	<p>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.</p> <p>An actual recovery response may substitute for an operational exercise.</p>	<p>Examples of evidence may include, but are not limited to, dated documentation of:</p> <ul style="list-style-type: none"> • 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-009-7 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-009-7 Table R3 – Recovery Plan Review, Update and Communication*.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BCS at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. PACS: and 2. EACMS <p>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>No later than 90 calendar days after completion of a recovery plan test or actual recovery:</p> <ol style="list-style-type: none"> 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. 	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.2	<p>High Impact BCS and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>Medium Impact BSC at Control Centers and their associated:</p> <ol style="list-style-type: none"> 1. PACS; and 2. EACMS <p>SCI hosting High or Medium Impact BCS at Control Centers or their associated:</p> <ul style="list-style-type: none"> • PACS; or • EACMS 	<p>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:</p> <ol style="list-style-type: none"> 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. 	<p>An example of evidence may include, but is not limited to, all of the following:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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.

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	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 applicable systems. OR The Responsible Entity has created recovery plan(s) for 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 applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.
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)	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	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 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 applicable system functionality according to R2 Part 2.2 within 18

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>OR</p> <p>The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>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)</p>	<p>used in the recovery of 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)</p> <p>OR</p> <p>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. (Requirement R2 Part 2.3)</p>	<p>The Responsible Entity has not tested a representative sample of the information used in the recovery of 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)</p> <p>OR</p> <p>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)</p>	<p>calendar months between tests. (Requirement R2 Part 2.2)</p> <p>OR</p> <p>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)</p>

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	<p>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)</p>	<p>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)</p> <p>OR</p> <p>The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)</p> <p>OR</p> <p>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</p>	<p>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)</p> <p>OR</p> <p>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)</p> <p>OR</p> <p>The Responsible Entity has not updated the recovery plan(s) or</p>	<p>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)</p>

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ability to execute the plan: (Requirement R3 Part 3.2) <ul style="list-style-type: none"> • Roles or responsibilities, or • Responders, or • Technology changes. 	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) <ul style="list-style-type: none"> • Roles or responsibilities, or • Responders, or • Technology changes. 	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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	<p>Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.</p> <p>Removal of reasonable business judgment.</p> <p>Replaced the RRO with the RE as a responsible entity.</p> <p>Rewording of Effective Date.</p> <p>Changed compliance monitor to Compliance Enforcement Authority.</p>	
3	12/16/09	<p>Updated Version Number from -2 to -3</p> <p>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.</p>	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
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.	

Version	Date	Action	Change Tracking
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	