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 — Information Protection

2. **Number:** CIP-011-3

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (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-011-3:

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 SCI.

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

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.

4.2.3.5. 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-002-5.1 identification and categorization processes.

5. "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.

6. Effective Dates: See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS.	Method(s) to identify information that meets the definition of BCSI.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BCSI from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BCSI; or • Repository or electronic and physical location designated for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS	Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 –Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • EACMS; • PACS; or • PCA	Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

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-011-3)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BCSI protection program (Requirement R1).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. (Requirement R2)

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	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Virtualization conforming changes	