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 final draft of the 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 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
45-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-~~3~~4

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

~~3.~~4. **Applicability:**

~~3.1.~~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.

~~3.1.1~~4.1.1 **Balancing Authority**

~~3.1.2~~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:

~~3.1.2.1~~4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

~~3.1.2.1.1~~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

~~3.1.2.1.2~~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.

~~3.1.2.2~~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.

~~3.1.2.3~~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.

~~3.1.2.4~~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.

~~3.1.3~~4.1.3 **Generator Operator**

~~3.1.4~~4.1.4 **Generator Owner**

~~3.1.5~~4.1.5 **Reliability Coordinator**

~~3.1.6~~4.1.6 **Transmission Operator**

~~3.1.7~~4.1.7 **Transmission Owner**

~~3.2.~~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.

~~3.2.1~~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:

~~3.2.1.1~~4.2.1.1 Each UFLS or UVLS System that:

~~3.2.1.1.1~~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

~~3.2.1.1.2~~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.

~~3.2.1.2~~4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.3~~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.

~~3.2.1.4~~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.

~~3.2.2~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

~~3.2.3~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-~~3~~4:

~~3.2.3.1~~4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

~~3.2.3.2~~4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~3.2.3.3~~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.

~~4.2.3.5~~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~~-5.1a~~ identification and categorization processes.

~~1. **Effective Dates:** See Implementation Plan for CIP-011-3.~~

~~2. **Background:** Standard CIP-011 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 its documented processes, but it 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 BES. 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:~~

~~3.3.~~4.3. ~~":~~ Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part 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-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** — Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

- B. **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.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Requirements and Measures

R1. ~~**R1.**~~ Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~"~~Applicable Systems~~"~~ identified in *CIP-011-~~3~~4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-~~3~~4 Table R1 – Information Protection Program*. *[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~~4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the 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 identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High ~~i~~impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following:

CIP-011-~~3~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		• 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). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~3~~4 Table R2 – ~~BES Cyber Asset~~ 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~~4 Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Prior to the release for~~Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse ~~of applicable Cyber Assets that contain BCSI~~ (except for reuse within other systems identified in the ~~"~~Applicable Systems~~"~~ column~~), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.~~). • 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 (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) 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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable 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~~4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). ~~(~~ (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include processes for reuse to prevent the unauthorized retrieval of BCSI from ~~the BES Cyber Asset~~an Applicable System. (Part 2.1)	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System~~the BES Cyber Asset~~. (Part 2.1)	The Responsible Entity ~~has not~~neither documented ~~or~~ nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

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	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD	Virtualization Modifications	