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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal or informal comment period with ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

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):
None.

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 ~~or~~ 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 Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

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

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-011-3.

6. 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicable~~ility~~ Systems" column further defines 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.
- **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.
- **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.

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 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 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	BCSI ~~System information~~ pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS~~; and~~ ~~3. PCA~~ Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS~~; and~~ ~~3. PCA~~	Method(s)~~Process(es)~~ to identify BCSI.~~information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.~~	Examples of acceptable evidence include, but are not limited to, the following: • Documented ~~process(es)~~method(s) to identify ~~BES Cyber System Information~~BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify~~recognize~~ BCSI~~BES Cyber System Information~~; or • Storage locations identified for housing BCSI~~BES Cyber System Information~~ in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BCSI~~BES Cyber System Information~~ as identified in ~~Requirement R1~~ Part 1.1	Method(s) to protect and securely handle BCSI.~~prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal.~~	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to protect and securely handle BCSI during its lifecycle, including:~~prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information and key management program, retention in the Physical Security Perimeter).~~ o Electronic mechanisms, o Physical mechanisms, o Technical mechanisms, or o Administrative mechanisms • ~~BES Cyber System Information~~BCSI is handled in a manner consistent with the entity's documented procedure(s)~~and key management program, retention in the Physical Security Perimeter)~~.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.43	BCSIBES Cyber System Information as identified in Requirement R1 Part 1.1.	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk identification and assessment method(s) for the following:Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.3.1 Data governance and rights management; and Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information 1.3.2 Identity and access management; and At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information 1.3.3 Security management; and Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Implementation of the risk identification and assessment method(s) (1.3);Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4);Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Business agreements that include communication expectations and protocols for

		1.3.4 Application, infrastructure, and network security.	disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1);~~Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and~~ • Consideration made for data sovereignty, if any (1.3.1);~~Dated documentation of action plans and statuses of remediation and/or mitigation action items~~ • Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3); • Dated documentation of vendor's identity and access management program (1.3.2); and • Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).

1.4	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	Examples of evidence may include, but are not limited to, dated documentation of the following: • Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]); • Evidence of implementation (e.g., configuration files, command output, architecture documents); and • Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R1. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. *[Violation Risk Factor: Medium] [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 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 — Key Management Program			
Part	Applicability	Requirement	Measure
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R2~~3~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2~~3~~. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~3~~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	Prior to the release for reuse ~~or disposal~~ of applicable ~~BES~~ 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 ~~shall be sanitized or destroyed~~.	Examples of acceptable evidence include, but are not limited to, the following: • 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. • ~~Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal.~~ • ~~Records that indicate chain of custody was implemented.~~

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI~~BES Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. 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.

~~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.~~

~~1.3.~~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 Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

~~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~~ applicable ~~E~~entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority~~CEA~~ to retain specific evidence for a longer period of time as part of an investigation:

- ~~Each~~ The ~~Responsible~~ applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible~~ applicable ~~E~~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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. **Compliance Monitoring and Assessment Processes:** 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~

- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)	~~The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)~~ The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity ~~has~~ did not ~~documented or~~ implement~~ed~~ one or more ~~a~~ documented ~~BES Cyber System~~ information protection program(s). (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
~~R2~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~ When the Responsible Entity used a vendor's services for BCSI as identified in Requirement R1, Part 1.1, the Responsible Entity documented one or more electronic technical mechanisms to prevent unauthorized logical access to BCSI but did not implement electronic technical mechanisms to prevent unauthorized logical access to BCSI. (R2)	When the Responsible Entity used a vendor's services for BCSI as identified in Requirement R1, Part 1.1, Tthe Responsible Entity has did not documented or implemented electronic technical mechanisms to prevent unauthorized logical access processes forto BCSI key management program. (R2)
R~~3~~2	**Operations Planning**	**Lower**	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~~BES~~	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~~BES~~	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber System Information~~ from the BES Cyber Asset. (2~~3~~.1)	~~Cyber System Information~~ from the BES Cyber Asset. (2~~3~~.~~1~~2)	Asset Reuse and Disposal. (~~R3~~R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

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	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their ~~BES Cyber System Information~~BCSI.

~~*Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~