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

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 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-~~2~~3

3. Purpose: To prevent unauthorized access to BES Cyber System Information 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 ~~Special Protection System (SPS)~~ or Remedial Action Scheme (RAS) where the ~~SPS or~~ 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 ~~SPS or~~ RAS where the ~~SPS or~~ 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-~~2~~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-~~2~~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 "Applicability Systems" column ~~to~~ 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-~~2~~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-~~2~~3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.1	System information pertaining to: High ~~-~~Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA	~~Method~~Process(es) to identify 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 ~~method~~ process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • ~~Repository or electronic and physical~~ Storage locations identified ~~designated~~ for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~PACS~~	~~Procedure~~Method(s) to prevent unauthorized access to ~~for protecting and securely handling~~ BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during~~, including~~ storage, transit, use, and disposal~~-~~.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to ~~Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of~~ BES Cyber System Information (e.g., encryption of ~~; or~~ • ~~Records indicating that~~ BES Cyber System Information and key management program, retention in the Physical Security Perimeter)~~is handled in a manner consistent with the entity's documented procedure(s)~~.

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

1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 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: • 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; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

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.

R2. 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.

R3~~2~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

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

CIP-011-~~2~~3 Table R~~2~~3 – 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 Cyber Assets ~~that contain BES Cyber System Information~~ (except for reuse within other systems identified in the "Applicable Systems" column), ~~the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information 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 BES Cyber System Information 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 BES Cyber System Information.~~ 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-011-2 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 BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information 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 BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

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 Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance ~~Violation~~ Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	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)~~N/A~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**~~Lower~~Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						management program. (R2)
R~~2~~3	**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 BES Cyber System Information from the BES Cyber Asset. (~~2~~3.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (~~2~~3.~~2~~1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal. (R~~2~~3)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~Guideline and Technical Basis (attached).~~

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.

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.

~~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:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.)~~

~~can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for

quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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:
The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.