Standard Development Timeline

~~**Note**: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.~~

~~This revised draft corrects the text box size to display all of the text (none of the text was changed).~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted.~~

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706~~,~~ approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ -011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~~~[1]~~

2. In those jurisdictions where no regulatory approval is required, ~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	TBD	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.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

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

2. **Number:** CIP-011-1

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 BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~4.1.2~~ **Distribution Provider** that owns ~~**Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS~~ System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

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 ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~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 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 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 Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme 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.

~~4.2.3~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers~~ and Load-Serving Entities~~**~~: All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-~~002-5~~011-1:

~~4.2.4.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3 ~~In nuclear plants, the Systems~~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 identification and categorization processes.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

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 ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies, . . .**

~~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. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

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 ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

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.

~~Applicability Columns in Tables:~~

~~Each table row ~~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 Bulk Electric System. 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:

Each table has an ~~applicability~~“Applicable Systems” column to further define the scope of systems to which a specific requirement row applies~~ to BES Cyber Systems and associated Cyber Assets. ~~. 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 ~~applicability~~“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 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **~~Associated ~~Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column~~. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **~~Associated ~~Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity~~ in the applicability column~~.

- ~~Associated~~ **Protected Cyber Assets ~~–~~(PCA)** ~~–~~ Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column.~~

Rationale – R1:

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

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement ~~an~~, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable ~~items~~requirement parts in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~.]~~].*

M1. Evidence for the information protection program must include the applicable ~~items~~requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	~~One or more documented and implemented methods~~Methods to identify information that meets the definition of BES Cyber System Information.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to~~,~~: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~it~~BES Cyber System Information as ~~BES Cyber System Information;~~ 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 ~~designated~~ electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection* (e.g., confidential, public, internal use only, etc.) *This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	~~One or more documented~~Procedures for protecting and ~~implemented procedures for~~securely handling BES Cyber System Information, including storage, transit, and use.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or ~~•~~ Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure~~; or~~ ~~• Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information.~~ • (s).
Reference to prior version: *CIP-003-3, R4; ~~CIP-003-3 R5.3~~*		**Change Rationale:** *The SDT ~~removed~~changed the language ~~to~~from "protect" information to "Procedures for protecting and ~~replaced it with "~~securely handling" to clarify the protection that is required.*	

~~CIP-011-1 Table R1 – Information Protection~~

~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirement~~	~~Measure~~
~~1.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~At least once every calendar year, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.~~	~~Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.~~
~~Reference to prior version:~~ *~~CIP-003-3, R4.3~~*		**~~Change Rationale:~~** *~~No significant changes.~~*	

Rationale – 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.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable ~~items~~requirement parts in *CIP-011-1 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 ~~items~~requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	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: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except ~~in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset~~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~~.~~ ~~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, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.~~ data storage media.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Records ~~of~~tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information~~;~~ such as clearing, purging, or destroying; or • ~~If removed from~~Records tracking actions such as encrypting, retaining in the Physical Security Perimeter ~~prior to action taken~~or other methods used to prevent unauthorized retrieval of ~~information, a chain of custody record that was maintained.~~ • BES Cyber System Information.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	Requirements	Measures
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	Requirements	Measures

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	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: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~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. ~~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 shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.~~	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of ~~a~~ an applicable Cyber Asset~~;~~. • ~~Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or~~ • ~~If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.~~

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

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 ~~Compliance Enforcement Authority~~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 ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years ~~or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- 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 ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.~~	~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information and one or more handling procedures for BES Cyber System Information, but has failed to assess adherence periodically as stated in Part 1.3, to its BES Cyber System Information protection program.~~	~~The Responsible Entity has not implemented a BES Cyber System Information protection program.~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program, but has not implemented one or more methods to identify BES Cyber System Information~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~protection program, but has not implemented one or more procedures for handling BES Cyber System Information.~~
~~R2~~	~~Operations Planning~~	~~Lower~~	~~N/A~~	~~The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.~~	~~The Responsible Entity has documented one or more processes, including both reuse and disposal, to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Assets, but the Responsible Entity either failed to take action to prevent the unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the~~	~~The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset.~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
					~~data storage media.~~	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

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. Furthermore,

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’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:

~~***Assumptions:***~~ 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. ~~The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.~~

~~While separating BES Cyber System Information into~~Identifying separate classifications of BES Cyber System Information is not specifically required~~ as it was in version 4~~. However, a Responsible Entity maintains ~~that~~the flexibility to do so if ~~desired~~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. ~~Topics that are appropriate for information handling~~ R1.2 requires one or more procedures ~~include access, sharing, copying, transmittal, distribution,~~for the protection and ~~disposal or destruction of~~ secure handling BES Cyber System Information~~.~~, including storage, transit, and use.

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.

~~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, it must be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~