

## Standard Development Timeline

*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).

**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.

### Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-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 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706, approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

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

## Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, 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.<sup>1</sup>
2. In those jurisdictions where no regulatory approval is required, Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, 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.

---

<sup>1</sup> 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 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 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 or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.
    - 4.2.2 **Distribution Provider:** One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:
      - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- 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 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities:** All BES Facilities.

**4.2.4 Exemptions:** The following are exempt from Standard CIP-002-5:

- 4.2.4.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.4.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.4.3** In nuclear plants, 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.

**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 common subject matter.

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 necessary in their documented processes, but they 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.

#### **Applicability Columns in Tables:**

Each table row has an applicability column to further define the scope 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 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** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding 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** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding 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 information protection program that includes each of the applicable items 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 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 Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, <ul style="list-style-type: none"> <li>• Indications on information (e.g., labels) that identify it as BES Cyber System Information;</li> <li>• Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or</li> <li>• Repository or designated electronic and physical location.</li> </ul>
<b>Reference to prior version:</b> CIP-003-3, R4; CIP-003-3, R4.2		<b>Change Rationale:</b> <i>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.</i>	

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 Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented procedures for handling BES Cyber System Information, including storage, transit, and use.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> <li>Records indicating that BES Cyber System Information is handled in a manner consistent with the entity’s documented procedure; or</li> <li>Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information.</li> </ul>
<b>Reference to prior version:</b> CIP-003-3, R4; CIP-003-3 R5.3		<b>Change Rationale:</b> <i>The SDT removed the language to “protect” information and replaced it with “handling” to clarify the protection that is required.</i>	

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.
<b>Reference to prior version:</b> <i>CIP-003-3, R4.3</i>		<b>Change Rationale:</b> <i>No significant changes.</i>	

**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 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 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 Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	<p>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), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset.</p> <p>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.</p>	Evidence may include, but is not limited to: <ul style="list-style-type: none"> <li>Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information; or</li> <li>If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained.</li> </ul>
<b>Reference to prior version:</b> CIP-007-3, R7.2		<b>Change Rationale:</b> <i>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.</i>	

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.2	<p>High Impact BES Cyber Systems</p> <p>Medium Impact BES Cyber Systems</p> <p>Associated Physical Access Control Systems</p> <p>Associated Electronic Access Control or Monitoring Systems</p> <p>Associated Protected Cyber Assets</p>	<p>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.</p> <p>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.</p>	<p>Evidence may include, but is not limited to:</p> <ul style="list-style-type: none"> <li>• Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset;</li> <li>• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of a an applicable Cyber Asset;</li> <li>• Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or</li> <li>• If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.</li> </ul>

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
		<p><b>Change Rationale:</b> <i>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.</i></p> <p><i>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.</i></p>	



## 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 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 may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for 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 specified above, whichever is longer.
- The Compliance Enforcement Authority 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
<b>R1</b>	<b>Operations Planning</b>	<b>Medium</b>	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.
<b>R2</b>	<b>Operations Planning</b>	<b>Lower</b>	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

### 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.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. 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 separate classifications is not required as it was in version 4, a Responsible Entity maintains that flexibility if desired. 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.

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 procedures include access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

### Requirement R2:

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. 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.