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).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-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. This version (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.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the 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, the standards shall become effective on the first day of the seventh 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 Application Guidelines Section of the Standard.

A. Introduction

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

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

3. **Purpose:** Standard CIP-011-1 requires that Responsible Entities have protection controls in place to protect BES Cyber System Information.

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 that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 **Interchange Coordinator**

4.1.6 **Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 **NERC**

4.1.8 **Regional Entity**

4.1.9 **Reliability Coordinator**

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 The following are exempt from Standard CIP-011-1:

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.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

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*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

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 specific elements required 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 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 infer any 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.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the 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.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. 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.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. 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 or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The intent of the information protection processes is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes:

Requirement R4.1 was moved to the definition of BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively 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	Applicability	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 Associated Protected Cyber Assets	One or more methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information.
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. 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	**Part**	**Part**	**Part**
1.2	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	Access control and handling procedures for BES Cyber System Information.	Evidence may include, but is not limited to: • Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process; • Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; • Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to “protect” information and replaced it with “Implement handling and access control” to clarify the protection that is required.*	

<table>
<tr><th colspan="4">CIP-011-1 Table R1 – Information Protection</th></tr>
<tr><th>Part</th><th>Part</th><th>Part</th><th>Part</th></tr>
<tr><td>1.3</td><td>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</td><td>Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.</td><td>Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP-003-3 R4.3</i></td><td colspan="2"><b>Change Rationale:</b> <i>No significant changes</i></td></tr>
</table>

Rationale – R2:

The intent of the media reuse and disposal processes is to prevent the unauthorized dissemination of BES Cyber System Information upon media 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 – Media 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 – Media Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

<table>
<tr><th colspan="4">CIP-011-1 Table R2 – Media Reuse and Disposal</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>2.1</td><td>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</td><td>Prior to the release for reuse of BES Cyber Asset media[2], the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.</td><td>Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b>
<i>CIP-007-3 R7.2</i></td><td colspan="2"><b>Change Rationale:</b> <i>(FERC Order 706 - p. 631) Consistent with FERC Order 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></td></tr>
</table>

[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.

<table>
<tr><th colspan="4">CIP-011-1 Table R2 – Media Reuse and Disposal</th></tr>
<tr><th>Part</th><th>Applicability</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>2.2</td><td>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</td><td>Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.</td><td>Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was purged or destroyed prior to its disposal.</td></tr>
<tr><td colspan="2"><b>Reference to prior version:</b> <i>CIP-007-3 R7.1</i></td><td colspan="2"><b>Change Rationale:</b> <i>Consistent with FERC Order 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>
<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></td></tr>
</table>

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

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 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 found compliant 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
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented one or more BES Cyber System Information protection processes that include one or more methods to identify BES Cyber System Information and one or more access control and handling procedures for BES Cyber System Information, but has failed to assess adherence, either initially upon the effective date of the standard or periodically, to its BES Cyber System Information protection processes.	The Responsible Entity has not implemented one or more BES Cyber System Information protection processes. OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more access control and handling

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures for BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the media disposal or reuse processes, including the recording of the media purge or destruction, were not followed.	The Responsible Entity has not documented or implemented any media disposal or reuse process to prevent the unauthorized retrieval of BES Cyber System Information from the media.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

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

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, responsible entities still have the flexibility to do this if they so desire. As long as the entity's information protection program includes all required elements, additional classification levels can be created that go above and beyond the requirements.

This requirement is not intended to 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. Information handling procedures should detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into 4 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, 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 which 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 this 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 should be properly erased using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.