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 the *Version 5 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	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the 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 — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** Standard CIP-005-5 requires the identification of all Electronic Access Points on the Electronic Security Perimeter(s), the protection of the communication through those points, and specific protections for interactive user remote access.

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
- 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 Exemptions: The following are exempt from Standard CIP-005-5

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.

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-005-5 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 each 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 each 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.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **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 for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.3	Electronic Access Points at High Impact BES Cyber Systems Electronic Access Points at Medium Impact BES Cyber Systems with External Routable Connectivity.	Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only explicit access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005 R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP.*	
1.4	Electronic Access Points that use dial-up access for non-Interactive Remote Access at High Impact BES Cyber Systems Electronic Access Points that use dial-up access for non-Interactive Remote Access at Medium Impact BES Cyber Systems.	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to a documented process identified in Requirement R1, Part 1.4 that describes how the Responsible Entity is providing authenticated access through each dial up Electronic Access Point.
Reference to prior version: *CIP-005 R2.3*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure", which is that the BES Cyber System should not be directly accessible with a phone number only*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.5	Electronic Access Points with External Routable Connectivity at High Impact BES Cyber Systems Electronic Access Points with External Routable Connectivity at Medium Impact BES Cyber Systems at Control Centers.	A documented method for detecting malicious communications at each EAP.	Evidence may include, but is not limited to: • Configuration files of an intrusion detection systems deployed at an EAP • Logs that were generated by an intrusion detection system • Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (*intrusion detection systems / intrusion protection systems*) a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Remote Access Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Note that a UserID is not considered an authentication factor.
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

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.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For 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 and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access OR The Responsible Entity did not establish Electronic Access Points to control and secure access to its BES Cyber Systems OR The Responsible Entity did not establish explicit inbound and outbound access permissions at each identified EAP that utilizes routable protocols OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not perform authentication before establishing connectivity with the BES Cyber System for an EAP that uses dial-up access OR The Responsible Entity did not deploy methods to detect malicious communications.
R2	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not implement an Intermediate Device between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005 R1 requires that BES Cyber Systems must be segmented from other systems of differing trust levels by requiring controlled electronic access points between the different trust zones. ESP's also are used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capabilities.

BES Cyber Systems are to be protected by Electronic Access Points (EAP's) that control traffic into and out of the BES Cyber System. Responsible Entities (RE's) should know what traffic needs to cross an EAP and document those justifications and insure the EAP's limit the traffic to only those known, justified communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

This requirement applies only to communications for which 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols and dialup modems. Direct serial, non-routable connections are not included.

The intent of securing dialup connectivity is to prevent situations where connectivity is established directly to the BES Cyber Asset with only a phone number. If a dialup modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is not functioning as an Electronic Access Point. The requirement calls for some form of authentication of the calling party when connectivity is granted to the BES Cyber Asset. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).