Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~7~~8

3. **Purpose:** To ~~manage electronic access to~~ protect BES Cyber Systems ~~by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems~~(BCS) against compromise ~~that could lead to~~ by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

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

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 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 RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~7~~8:

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

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. 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.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~**5. Effective Date:** See Implementation Plan for Project 2019-03.~~

~~**6. Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the 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**~~**:**

4.3. Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.~~

- ~~**High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**High Impact BES Cyber Systems with Dial-up Connectivity –** Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**High Impact BES Cyber Systems with External Routable Connectivity –** Only applies to high 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.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**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.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 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 requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA	~~All applicable Cyber Assets~~Applicable Systems connected to a network via a routable protocol ~~shall reside within a defined~~must be protected by an ESP.	~~An example~~Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
			configuration).
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or	An example of evidence may include, but is not limited to, documentation that malicious routable protocol

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
		leaving an ESP.	communications detection methods (e.g., intrusion detection system, application layer firewall, etc.) are implemented.
1.~~2~~6	High ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS at Control Centers and their associated~~:~~ PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. Time-sensitive communication of Protection Systems.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~network diagrams showing all external routable communication paths~~documentation of methods used to protect the confidentiality and integrity of the ~~identified EAPs.~~ data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

~~CIP-005-7 Table R1 – Electronic Security Perimeter~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~1.3~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~
~~1.4~~	~~High Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~	~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~
~~1.5~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	~~An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-~~7~~8 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 requirement parts in *CIP-005-~~7~~8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	~~For all~~Permit Interactive Remote Access~~, utilize~~ (IRA), if any, only through an Intermediate System~~ such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~.	Examples of evidence may include, but are not limited to, network diagrams~~ or~~, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~Intermediate System(s) used to access an Applicable System in Part 2.1	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption ~~initiates~~) initiate and ~~terminates.~~ terminate.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for ~~all Interactive Remote Access sessions~~IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Example of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ ~~•~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ ~~•~~ PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~)~~, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g., connection tables or rule hit

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			counters in a firewall, or user activity monitoring) or open ports (e.g.~~,~~ netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ ~~such as:~~ • ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~).

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~ high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
			firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for ~~both inbound and outbound~~permitting communications. (Part 1.~~5)~~2)	The Responsible Entity did not document one or more processes for *CIP-005-~~6~~8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not ~~have all applicable Cyber Assets~~protect the Applicable Systems connected to ~~a~~the network ~~via a~~with routable protocol ~~within a defined Electronic Security Perimeter (ESP). (~~with an ESP. (Part 1.1) OR ~~External Routable Connectivity through the ESP was not through an identified EAP. (1.2)~~ ~~OR~~ The Responsible Entity did not ~~require inbound and outbound access permissions~~permit only needed communications and deny all other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~access~~communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by ~~default.~~ ~~(~~implementing methods to permit only needed network accessibility to Management Interfaces for Applicable Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing ~~dial~~Dial-up ~~connectivity with the applicable Cyber Assets, where technically feasible.~~ ~~(~~Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~ IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ (SCI.* (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS ~~(~~or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS ~~(3.2~~or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote connections for EACMS ~~(~~or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ (SCI.* (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS ~~(~~or SCI supporting EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project ~~2019-03~~2016-02
- CIP-005-~~7~~8 Technical Rationale

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	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Modified by Project 2016-02.	