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 initial draft of 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
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System -Logical Isolation~~Electronic Security Perimeter(s)~~

2. **Number:** CIP-005-87

3. **Purpose:** To ~~manage electronic access to~~protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication.~~by specifying a controlled Electronic Security Perimeter~~ to reduce the likelihood of misoperations or instability in the BES. ~~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 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-005-8~~7~~:

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 Perimeterslogically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Ssystems associated with communication links between Cyber Assets, or Virtual Cyber Assets, or SCI performing logical isolation 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.

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

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted 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.

5. Effective Date: See Project 2016-02 Virtualization Implementation Plan. for Project 2019-03.

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:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row 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.

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-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. *[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-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); ~~1.~~2. Physical Access Control Systems (PACS) hosted on SCI; and ~~2.~~3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. PCA; ~~1.~~2. PACS hosted on SCI; and ~~2.~~3. EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP~~ Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	~~An e~~Examples of evidence may include, but is not limited to, ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP~~documentation that includes the configuration of systems ~~that enforce electronic access control and logical isolation and document business need~~ such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration);~~.~~ that enforces electronic access control and logical isolation and documents the business need.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS ~~High Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~ Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	~~An e~~Examples of evidence may include, but is not limited to, ~~network diagrams showing all external routable communication paths and the identified EAPs~~documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS connected to a network via routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: • confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other nonprogrammable communication components, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE). ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of e~~Evidence may include, but is not limited to, architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption)~~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~~.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and ~~1.~~3. EACMS hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated: • PCS; • PACS; or • EACMS	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~systems, per system capability.	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.

CIP-005-87 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS at Control Centers and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PCA; • PACS, or • EACMS ~~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~~ D~~d~~etect~~ing~~ known or suspected malicious Internet Protocol (IP) communications ~~for both inbound and outbound communications~~entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~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-005-8~~7~~ 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-005-8~~7~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-87 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • PCA SCI with IRA hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS~~.~~ Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Ensure that ~~authorized~~ IRA is through an Intermediate System. ~~For all Interactive Remote Access, utilize 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, or Management Systems reports that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access applicable systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where ~~encryption~~ confidentiality and

CIP-005-87 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~High Impact BES Cyber Systems and their associated:~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	integrity controls initiate~~s~~ and terminate~~s~~.
2.3	Intermediate Systems used to access applicable systems of Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~2. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~3. PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents 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.

CIP-005-87 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access ~~External Routable Connectivity~~ and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access 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 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.

CIP-005-87 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access~~External Routable Connectivity~~ and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	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-005-87 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Intermediate Systems used to access applicable systems of Part 2.1	Implement for applicable systems as follows: **2.6.1.** Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	Examples of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

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 and PACS*. *[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 and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS	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~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable~~	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

CIP-005-87 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Connectivity~~ERC SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS		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 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 Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.~~for both inbound and outbound communications. (1.5)~~	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~ 8 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. ~~have all applicable Cyber Assetssystems connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). protected by logical isolation~~ (Requirement R1 Part 1.1) OR The Responsible Entity did not ~~protect~~implement, for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability ~~the Management Systems or Management Interfaces or applicable systems per Requirement R1, Part 1.2External Routable Connectivity through the ESP was not through an identified EAP.~~ (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				nonprogrammable communication components ~~protect confidentiality and integrity of the data traversing communications links per Requirement R1, Part 1.3.The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default.~~ (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing D~~d~~ial-up ~~c~~Connectivity with the applicable ~~Cyber Assets~~systems~~, where technically feasible~~. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	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;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	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) (Requirement R2 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) (Requirement R2 Part 2.5).	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) (Requirement R2 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) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-~~8~~7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS, ~~and~~ SCI, and ~~-~~Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by	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, ~~and~~ SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (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
		Part 3.2 for EACMS~~, and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS~~, and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and ~~and~~ EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Virtualization Implementation Plan." ~~for Project 2019-03~~
- CIP-005-87 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	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	