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~~ second 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
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 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~~29–~~September 16~~October 11, 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-005-8

3. **Purpose:** 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 to~~ reduce the likelihood of misoperations 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:

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

4.2.3.2. Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BCS or~~

~~Shared Cyber Infrastructure (SCI)~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber ~~s~~Systems, associated with communication links, between the Cyber ~~Assets~~Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that ~~, Virtual Cyber Assets, or SCI performing logical isolation that~~ extends to one or more geographic locations.

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.

4.2.3.5. 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 BCS 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~~ part 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~~ Modification 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-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)*. *[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-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS ~~connected to a network via a routable protocol~~ and their associated ~~:~~ Protected Cyber Asset (PCA)~~;~~ ~~(VCA) Physical Access Control Systems (PACS) hosted on SCI; and~~ ~~Electronic Access Control or Monitoring System (EACMS) hosted on SCI~~ ~~•~~Medium Impact BCS ~~connected to a network via a routable protocol~~ and their associated PCA~~:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~	Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies ~~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).~~ Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as: • Electronic Access Point (EAP) configuration or policies; • 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 an ESP ~~electronic access control and logical isolation~~ and documents the business need.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI identified independently ~~hosting~~supporting an Applicable System from Part 1.1. ~~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 enforces an ESP for the Applicable Systems in Part 1.1. ~~perform logical isolation for a High Impact BCS~~ ~~EACMS that perform logical isolation for a Medium Impact BCS~~	~~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~~deny all other communications. ~~1.2.3. Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.~~	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control and ESP~~logical isolation~~ such as: • Logical~~ly 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, or~~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-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~

Part	Applicable Systems	Requirements	Measures
1.3.	SCI identified independently supporting an Applicable System from Part 1.1.	Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control such as: • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration); • Logical network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated out-of-band network for dedicated Management Interfaces.

CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)

Part	Applicable Systems	Requirements	Measures
1.4~~3~~	High Impact BCS Medium Impact BCS at Control Centers ~~Impact BCS and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~Medium Impact BCS connected to a network via routable protocol and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~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~~	Protect the data traversing communication links used to span a single ESP between ~~, where the logical isolationto spans a sindifferentmultiple~~ Physical Security Perimeters (PSP)~~,~~ through the use of: • confidentiality and integrity controls (such as encryption), or • ~~Physical~~ physical controls that restrict access to the cabling and other nonprogrammable communication components in those instances when such cabling and components are located outside of a ~~Physical Security Perimeter~~PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. ~~excluding~~ time-sensitive protection or control functions between intelligent electronic devices. ~~(e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).~~	An example of ~~E~~evidence may include, but is not limited to, ~~architecture~~ documentation~~s~~ ~~detailing the~~of methods used to protect the confidentiality and integrity of the data, such as: ~~(e.g., encryption).~~ • Configurations or policies used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.54	High Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI identified independently supporting an Applicable System above. ~~with Dial-up Connectivity hosting High or Medium Impact BCS or their associated:~~ ~~PCS;~~ ~~PACS; or~~ ~~EACMS~~	Perform authentication when establishing Dial-up Connectivity with ~~a~~Applicable ~~s~~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-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6~~5~~	EACMS that enforces an ESP for the Applicable Systems in Part 1.1. at Control Centers ~~High Impact BCS and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~Medium Impact BCS at Control Centers and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~SCI at Control Centers hosting High or Medium Impact BCS or their associated:~~ ~~PCA;~~ ~~PACS, or~~ ~~EACMS~~	Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP ~~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 IRA and vendor 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 Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 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-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BCS and their associated: • PCA Medium Impact BCS with ~~Interactive Remote Access (IRA)~~ERC and their associated: • PCA EACMS that enforces an ESP for the Applicable Systems in Part 1.1. SCI identified independently supporting an Applicable System above ~~SCI with IRA hosting High or Medium Impact BCS or their associated:~~	~~Ensure that~~Permit authorized IRA, if any, only ~~is~~ through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.

	~~• PCA;~~ ~~• PACS; or~~ ~~• EACMS~~ ~~Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PCA;~~ ~~• PACS; or~~ ~~EACMS~~		
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 or configuration detailing where confidentiality and integrity controls initiate and terminate.
2.3	Intermediate Systems used to access Applicable Systems of Part 2.1	Require multi-factor authentication 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.
2.4	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System above ~~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 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.

2.5	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System above~~e~~ ~~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 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 IRA and system-to-system remote access.
2.6	Intermediate Systems used to access ~~a~~Applicable ~~s~~Systems of Part 2.1	Implement for ~~a~~Applicable ~~s~~Systems as follows: **2.6.1.** Restrict VCAs of Intermediate Systems to only share CPU and memory with other	Examples of evidence may include, but are not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS.

		Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and ~~a~~Applicable ~~ms~~ Systerms of Part 2.1.	• 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-005-8 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-005-8 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 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ~~External Routable Connectivity (~~ERC~~)~~ SCI identified independently supporting an Applicable System above ~~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 BCS EACMS and PACS associated with Medium Impact BCS with ERC	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

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
	SCI identified independently supporting an Applicable System above ~~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~~		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 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~~ESP required by Part 1.1 or Part 1.2.2.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – ~~Logical Isolation~~ESP*. (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~~ESP all other communications. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems, per system capability (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~~ESP 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)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not implement a method to protect the data traversing communication links, where the ~~logical isolation~~ESP 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 (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the applicable systems. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented	The Responsible Entity did not implement processes	The Responsible Entity did not implement processes	The Responsible Entity did not implement processes

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	for one of the applicable items for Requirement Parts 2.1 through 2.3.	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 IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).	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 IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including 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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Intermediate Systems, per 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 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, 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 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, SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity had method(s) as required by Part 3.2 for EACMS, 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).	initiated remote connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, 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 EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of	required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			SCI (Requirement R3 Part 3.1). 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."
- CIP-005-8 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	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	