NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-005-8 – Cyber Security – Electronic Security Perimeter(s)

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Name of Registered Entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		

*CIP-005-8 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-005-8 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

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 – 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-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more process(es) which require applicable Cyber Systems connected to a network via a routable protocol to be protected by a defined ESP.
	Verify each Cyber Asset of an Applicable System that is connected to a network via a routable protocol resides within a defined ESP.
	For each defined ESP, verify the identification of any associated PCA.

Notes to Auditor:

1. This Part is applicable to all high and medium impact BES Cyber Systems and their associated PCA regardless of External Routable Connectivity.
2. Those Cyber Assets that are part of a high or medium impact BES Cyber System that are not connected to a network via a routable protocol need not reside within a defined ESP.
3. For Cyber Assets that are part of a high or medium impact BES Cyber System that do not reside within a defined ESP, the absence of a connection to a network via a routable protocol will be verified.
4. The reason to identify an ESP without External Routable Connectivity is to identify the PCA associated with the ESP.
5. In order to verify that each Cyber Asset residing within a defined ESP has been identified as either a BES Cyber Asset or as a PCA, it may be necessary to examine the ESP and conduct an inventory of network connections within the ESP.
6. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same defined ESP.

Auditor Notes:

R1 Part 1.2

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 configuration).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which 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.
	Verify that all External Routable Connectivity is through an identified EAP.
	For each defined ESP without an identified EAP, verify that no External Routable Connectivity exists.

Auditor Notes:

R1 Part 1.3

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 accessability 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).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.
	For each Applicable System, verify only needed network accessibility to Management Interfaces of Applicable Systems, per system capability are permitted.

Auditor Notes:

R1 Part 1.4

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated PCA Medium impact BCS Band their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, per system capability.
	For each Cyber Asset of an Applicable System, verify authentication is performed when establishing a dial-up connection, or that the system is incapable of authentication.
Note to Auditor: If the Responsible Entity does not have or does not allow Dial-up Connectivity, the Responsible Entity is not required to document one or more processes to perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets. It is sufficient to verify that the Responsible Entity does not have Dial-up Connectivity.	

Auditor Notes:

R1 Part 1.5

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
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 leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.
	For each Applicable System, verify the Responsible Entity has implemented one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.

Auditor Notes:

R1 Part 1.6

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	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.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the 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).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.6

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include one or more methods for protecting 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 ii. Time-sensitive communication of Protection Systems.
	For each Applicable System, verify the Responsible Entity has implemented one or more methods for protecting 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 ii. Time-sensitive communication of Protection Systems.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each 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.

R2 Part 2.1

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 and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Report Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which permit IRA, if any, only through an Intermediate System.
	Verify all IRA utilizes an Intermediate System, or that the system is incapable of utilizing an Intermediate System.
	Verify that the Cyber Asset initiating IRA does not directly access an applicable Cyber Asset, or that or that the system is incapable of not directly accessing an applicable Cyber Asset.
	If a system is incapable of utilizing an Intermediate System or of not directly accessing an applicable Cyber Asset, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.2

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
	Verify the Responsible Entity has documented one or more processes which Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.

Auditor Notes:

R2 Part 2.3

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
	Verify all IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System require multi-factor authentication, or that the system is incapable of requiring multi-factor authentication.
	If a system is incapable of requiring multi-factor authentication, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.4

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS and their associated PCA Medium 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 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 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).
	Verify all active vendor remote access sessions (including IRA and system-to-system remote access) can be determined, per system capability.
	If a system is incapable of determining all active vendor remote access sessions, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.5

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS and their associated PCA Medium 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 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).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods for disabling active vendor remote access sessions (including IRA and system-to-system remote access).
	Verify all active vendor remote access sessions (including IRA and system-to-system remote access) can be disabled
	If a system is incapable of disabling all active vendor remote access sessions, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.6

CIP-005-8 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.6

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.
	Verify the Responsible Entity implemented one or more processes to prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.
	If a system is incapable of preventing an Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.7

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.7

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to include routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.
	Verify the Responsible Entity implemented one or more processes to include Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.
	If a system is incapable of including Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP, verify that compensating measures are implemented.

Auditor Notes:

R3 Supporting Evidence and Documentation

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, 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-005-8 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.

R3 Part 3.1

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with 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.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R3, Part 3.1
This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods to determine authenticated vendor-initiated remote connections.
	Verify the Responsible Entity implemented one or more methods to determine authenticated vendor-initiated remote connections by implementing the documented process:

Note to Auditor:
When implementing the documented process, it should be either:

- Continuously, providing connection information in real time. In this case evidence of the continuous monitoring should be reviewed to verify the capability.
- On demand, initiated as needed by the Responsible Entity. In this case, a live demonstration or other means of verification of the ability may be used.

Auditor Notes:

R3 Part 3.2

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with 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 firewall; or physically disconnecting a network cable to prevent a reconnection.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods to terminate authenticated vendor-initiated remote connections.
	Verify the Responsible Entity has documented one or more processes which have one or more methods to control the ability to reconnect authenticated vendor-initiated remote connections.
	Verify the Responsible Entity has implemented one or more methods for terminating authenticated vendor-initiated remote connections by implementing the documented process.
	Verify the Responsible Entity has implemented one or more methods for controlling the ability to reconnect authenticated vendor-initiated remote connections by implementing the documented process.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-005-8 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
V1	02/28/2024		Initial Draft