NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-005-5 – 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:	Registered name of 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	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		

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 approved version of the Reliability Standards, 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			
P1.1			
P1.2			
P1.3			
P1.4			
P1.5			
R2			
P2.1			
P2.2			
P2.3			

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-005-5 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 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-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example 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.

Registered Entity Response (Required):
Question: Is R1 Part 1.1 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and

e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all devices (BES Cyber Assets and Cyber Assets) which comprise the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. An indication of whether the device is connected to a network via a routable protocol.
   b. If the device is connected to a network via a routable protocol, identification of the ESP protecting each device.
3. For each ESP identified in response to Evidence Set 2 Item 2 above, provide the following evidence:
   a. Identification of each Cyber Asset residing within the ESP.
   b. Classification of each Cyber Asset residing within the ESP:
      - Cyber Asset that is a component of a High Impact BES Cyber System;
      - PCA associated with a High Impact BES Cyber System;
      - Cyber Asset that is a component of a Medium Impact BES Cyber System; or
      - PCA associated with a Medium Impact BES Cyber System.

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-005-5, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.

	Verify the entity has documented one or more processes which address this Part.
	For each sampled BES Cyber System, verify each associated BES Cyber Asset and Cyber Asset that is connected to a network via a routable protocol resides within a defined ESP.
	For each ESP associated with a sampled BES Cyber System, verify all devices residing within the ESP are identified.
	For each ESP associated with a sampled BES Cyber System, verify each device residing within the ESP is properly classified as: • A component of the highest-rated BES Cyber System within the ESP, or • A PCA associated with the highest-rated BES Cyber System within the ESP.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. In order to verify that each Cyber Asset residing within the ESP has been identified as either a BES Cyber Asset or as a PCA, it may be necessary to physically examine the ESP and conduct an inventory of network connections to the ESP.

Auditor Notes:

R1 Part 1.2

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	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).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

Registered Entity Response (Required):
Question: Is R1 Part 1.2 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all devices (BES Cyber Assets and Cyber Assets) which comprise the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
    a. An indication of whether the device is connected to a network via a routable protocol.
    b. If the device is connected to a network via a routable protocol, identification of the ESP protecting each device.
3. For each ESP identified in response to Evidence Set 2 Item 2 above, provide the following evidence:
    a. Identification of each Electronic Access Point associated with the ESP.
    b. For each Cyber Asset residing within the ESP:
        i. Identification of the Cyber Asset;
        ii. Identification of each network interface;
        iii. Identification of the routable network, if any, to which each network interface is connected.

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-005-5, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	For each ESP associated with a sampled BES Cyber System, verify that all EAPs have been identified.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R1 Part 1.3

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

Registered Entity Response (Required):
Question: Is R1 Part 1.3 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this

sample set, provide the list of all devices (BES Cyber Assets and Cyber Assets) which comprise the BES Cyber System.

2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. An indication of whether the device is connected to a network via a routable protocol.
   b. If the device is connected to a network via a routable protocol, identification of the ESP protecting each device.
3. For each ESP identified in response to Evidence Set 2 Item 2 above, provide the following evidence:
   a. Identification of each Electronic Access Point (EAP) associated with the ESP.
4. For each EAP identified in response to Evidence Set 2 Item 3 above, provide the following evidence:
   a. The list of inbound access permissions, including the reason for granting access;
   b. The list of outbound access permissions, including the reason for granting access;
   c. Evidence that inbound and outbound access is denied by default.

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-005-5, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	Verify inbound and outbound access permissions are implemented.
	Verify each inbound and each outbound permission includes the reason for granting access.
	Verify inbound and outbound access is denied by default.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.

Note to Auditor:

1. If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal

operations, emergency operations, support, maintenance, and troubleshooting.

Auditor Notes:

R1 Part 1.4

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Registered Entity Response (Required):
Question: Is R1 Part 1.4 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:

Evidence Set 2:

1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all devices (BES Cyber Assets and Cyber Assets) which comprise the BES Cyber System.
2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
    a. An indication of whether the device is accessible via Dial-up Connectivity.
3. For each Cyber Asset accessible via Dial-up Connectivity identified in response to Evidence Set 2 Item 2 above, provide the following evidence:
    a. Evidence that authentication is performed when establishing Dial-up Connectivity.

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-005-5, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	For each Cyber Asset accessible via Dial-up Connectivity, verify authentication is performed when establishing a connection, or that an approved TFE covers the device.
	If a TFE is applicable to a device, verify the compensating measures identified by the TFE are in place.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R1 Part 1.5

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Registered Entity Response (Required):

Question: Is R1 Part 1.5 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.

☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of BES Cyber Systems to be used for the evidence requested below:
Evidence Set 2: 1. From the list of BES Cyber Systems provided in response to Evidence Set 1 Item 1, the Compliance

Enforcement Authority will select a sample of BES Cyber Systems. For each BES Cyber System in this sample set, provide the list of all devices (BES Cyber Assets and Cyber Assets) which comprise the BES Cyber System.

2. For each device identified in response to Evidence Set 2 Item 1 above, provide the following evidence:
   a. An indication of whether the device is connected to a network via a routable protocol.
   b. If the device is connected to a network via a routable protocol, identification of the ESP protecting each device.
3. For each ESP identified in response to Evidence Set 2 Item 2 above, provide the following evidence:
   a. Identification of each Electronic Access Point associated with the ESP.
4. For each EAP identified in response to Evidence Set 2 Item 3 above, provide the following evidence:
   a. Method(s) used to detect known or suspected malicious communications for both inbound and outbound communications.

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-005-5, R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	For each EAP, verify the entity has implemented at least one method for detecting known or suspected malicious communications for both inbound and outbound communications.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive 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-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	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.

Registered Entity Response (Required):
Question: Is R2 Part 2.1 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.

Evidence Set 1:

1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide:
   a. The name or other identification of the BES Cyber System,
   b. The name or other identification of the associated asset,
   c. The type of the associated asset,
   d. The impact rating of the BES Cyber System, and
   e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.
2. For each ESP identified in Evidence Set 1 Item 1, above, provide an indication of whether Interactive Remote Access is configured.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters for which Interactive Remote Access is configured to be used for the evidence requested below:

Evidence Set 2:

1. From the list of Electronic Security Perimeters for which Interactive Remote Access is configured provided in response to Evidence Set 1 Item 2, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters. For each Electronic Security Perimeter in this sample set, provide the following evidence:
   a. Documentation of the configuration of Interactive Remote Access for this ESP. This documentation should identify the Intermediate System(s) used, and how the Intermediate System(s) prevent direct access of an applicable Cyber Asset.

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-005-5, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in

	this list.
	Verify the entity has documented one or more processes which address this Part.
	Verify Interactive Remote Access is configured to utilize an Intermediate System, or that an approved TFE covers this circumstance.
	Verify no applicable Cyber Assets are directly accessible from assets outside an ESP, other than through an Intermediate System, or that an approved TFE covers this circumstance.
	If a TFE covers one or more of these issues, verify the compensating measures identified by the TFE are in place.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Part 2.2

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: • 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.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

Registered Entity Response (Required):
Question: Is R2 Part 2.2 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System, b. The name or other identification of the associated asset, c. The type of the associated asset, d. The impact rating of the BES Cyber System, and e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside. 2. For each ESP identified in Evidence Set 1 Item 1, above, provide an indication of whether Interactive

Remote Access is configured.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters for which Interactive Remote Access is configured to be used for the evidence requested below:
Evidence Set 2: 1. From the list of Electronic Security Perimeters for which Interactive Remote Access is configured provided in response to Evidence Set 1 Item 2, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters. For each Electronic Security Perimeter in this sample set, provide the following evidence: a. Documentation of the configuration of Interactive Remote Access for this ESP. This documentation should describe how encryption is employed for the Interactive Remote Access session, and the termination points of that encryption.

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-005-5, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	Verify all Interactive Remote Access utilizes encryption that terminates at an Intermediate System, or that an approved TFE covers this circumstance.
	If a TFE covers one or more of these issues, verify the compensating measures identified by the TFE are in place.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Part 2.3

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	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.

Registered Entity Response (Required):
Question: Is R2 Part 2.3 applicable to this audit? ☐ Yes ☐ No
If "No," why not?
☐ This entity is not responsible for compliance for any of the systems listed in the "Applicable Systems" column of the Table for this Part.
☐ Other: [Provide explanation below]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence Set 1: 1. List of all BES Cyber Systems identified as an Applicable System. For each BES Cyber System, provide: a. The name or other identification of the BES Cyber System,

b. The name or other identification of the associated asset,
c. The type of the associated asset,
d. The impact rating of the BES Cyber System, and
e. The name or other designation of all ESPs within which the BES Cyber Assets and Cyber Assets associated with the BES Cyber System reside.

2. For each ESP identified in Evidence Set 1 Item 1, above, provide an indication of whether Interactive Remote Access is configured.

Additional Evidence Requested:

In response to Evidence Set 1, above, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters for which Interactive Remote Access is configured to be used for the evidence requested below:

Evidence Set 2:

1. From the list of Electronic Security Perimeters for which Interactive Remote Access is configured provided in response to Evidence Set 1 Item 2, the Compliance Enforcement Authority will select a sample of Electronic Security Perimeters. For each Electronic Security Perimeter in this sample set, provide the following evidence:
   a. Documentation of the configuration of Interactive Remote Access for this ESP. This documentation should identify the authentication methods for all Interactive Remote Access sessions.

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-005-5, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicability of this Part to this entity. If the Part is not applicable, skip the remaining items in this list.
	Verify the entity has documented one or more processes which address this Part.
	Verify all Interactive Remote Access sessions require multi-factor authentication, or that an approved TFE

	covers this circumstance.
	If a TFE covers one or more of these issues, verify the compensating measures identified by the TFE are in place.
	If one or more of the "verify" steps above fails, a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-005-5 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

FERC Order No. 706
FERC Order No. 791

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Term	Acronym	Definition
BES Cyber Asset	BCA	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.
BES Cyber System		One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Control Center		One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
Cyber Assets		Programmable electronic devices, including the hardware, software, and data in those devices.
Dial-up Connectivity		A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.
Electronic Access Control or Monitoring Systems	EACMS	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.
Electronic Access Point	EAP	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter	ESP	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
External Routable Connectivity		The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Interactive Remote Access		User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
Intermediate System		A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
Protected Cyber Assets	PCA	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset.

Transient Cyber Asset		A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1v0	06/17/2014	Posted for Public Comment	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.