

**Reliability Standard Audit Worksheet for British Columbia**

CIP-005-5 – Cyber Security – Electronic Security Perimeter(s)

Reliability Standard Effective Date for BC: October 1, 2018

***The Compliance Monitor Administrator must complete this section***

**Registered Entity:** [Name & ACRO]

**WCR Number:** WCRXXXXX

**Compliance Assessment Date:** [Audit start date – audit end date]

**Compliance Monitoring Method:** [Audit Type]

**Applicable Function(s):** BA, DP, GO, GOP, TO, TOP

**Names of Auditors:**

Findings Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Req. | Finding | Summary and Documentation | Functions Monitored |
| [R1](#R1_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |
| [R2](#R2_Summary) |  |  | BA, DP, GO, GOP, TO, TOP |

|  |  |
| --- | --- |
| Req. | Areas of Concern |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Req. | Recommendations |
|  |  |
|  |  |
|  |  |

# **Subject Matter Experts**

Identify subject matter expert(s) responsible for this Reliability Standard. Insert additional lines if necessary.

**Registered Entity Response (Required):**

|  |  |  |  |
| --- | --- | --- | --- |
| **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.

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more process(es) which require all applicable Cyber Assets connected to a network via a routable protocol to reside within 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 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.
 |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which ensure all External Routable Connectivity is through an identified Electronic Access Point (EAP). |
|  | 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.  |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. |
|  | For each Applicable System, verify inbound and outbound access permissions are implemented. |
|  | For each Applicable System, verify each inbound and each outbound access permission includes the reason for granting access. |
|  | For each Applicable System, verify inbound and outbound access is denied by default. |
| **Note to Auditor:** Some vendor firewalls contain an implicit “deny” statement in the Access Control List (ACL). Vendor documentation of that configuration is a form of evidence to demonstrate the deny by default requirement within this Part. |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.4

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes to perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets, where technically feasible. |
|  | For each Cyber Asset of an Applicable System, verify authentication is performed when establishing a dial-up connection. |
|  |  |
| **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 they do not have Dial-up Connectivity. |

| **CIP-005-5 Table R1 – Electronic Security Perimeter** |
| --- |
| **Part** | **Applicable Systems** | **Requirements** | **Measures** |
| 1.5 | Electronic Access Points for High Impact BES Cyber SystemsElectronic 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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 1.5

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which include one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. |
|  | For each Applicable System, verify the Responsible Entity has implemented one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. |

**[Compliance Summary:](#R1)**

|  |
| --- |
| Finding Summary:Primary Documents Supporting Findings: |

**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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.1

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which require the utilization of an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. |
|  | Verify all Interactive Remote Access utilizes an Intermediate System. |
|  | Verify that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. |
|  |  |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.2

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which utilize encryption that terminates at an Intermediate System for all Interactive Remote Access sessions. |
|  | Verify all Interactive Remote Access utilizes encryption that terminates at an Intermediate System. |
|  |  |

| **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):**

Describe, in narrative form, how you meet compliance with this requirement.

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 Monitor Administrator):

|  |
| --- |
|  |
|  |
|  |

Compliance Assessment Approach Specific to Part 2.3

***This section to be completed by the Compliance Monitor Administrator***

|  |  |
| --- | --- |
|  | Verify the Responsible Entity has documented one or more processes which require multi-factor authentication for all Interactive Remote Access sessions. |
|  | Verify all Interactive Remote Access sessions require multi-factor authentication. |
|  |  |

**[Compliance Summary:](#R2)**

|  |
| --- |
| Finding Summary:Primary Documents Supporting Findings: |

**Auditor Notes:**

|  |
| --- |
|  |

**Revision History for RSAW**

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer(s)** | **Revision Description** |
| 3/4/2016 | Jennifer Salisbury, WECCJulie Blair, WECCWECC CIP SME | Intial version  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |