

[Registered Entity Name]

NERC ID: [NCRXXXXX]

CIP-012-1 – Cyber Security – *Communications between Control Centers*

[QX] [20XX] Guided Self-Certification Worksheet

# Instructions

1. Populate the cover page by adding your Registered Entity name, NERC compliance registry (NCR) number, and the quarter and year indicated for the Guided Self-Certification in Align.
2. Complete the tasks listed under Assessment Guidance. Only complete tasks listed for the Requirements in scope.
3. Log into Align and complete your Guided Self-Certification response.
4. Where random sampling is required, use an objective tool such as Microsoft Excel or random.org. If you have questions, reference NERC’s [Compliance Monitoring and Enforcement Manual](https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20Enterprise%20Compliance%20Monitoring%20and%20Enforcement%20Manual%20v6.pdf) (2021 Version 6, p. 151) or contact your Guided Self-Certification lead for assistance.
5. Submit the following to the Secure Evidence Locker (SEL):
	1. This completed worksheet; and
	2. The specific evidence annotated for the requested Requirements.
		1. Please use unique file names and identify which file(s) support each conclusion.
		2. Direct references and unique file names facilitate an expedited review of the Guided Self-Certification.
6. The Guided Self-Certification request in Align includes the monitoring period and the timeframe to perform the assessment and respond.
7. For the purpose of this document all capitalized terms have the meaning ascribed to them in the NERC *Glossary of Terms Used in NERC Reliability Standards* ([Available Here](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)) unless otherwise indicated.

# Requirement

The scope of this CIP-012-1 Guided Self-Certification is listed below:

|  |  |
| --- | --- |
| CIP-012-1 Requirement | In Scope |
| **R1** | *Requirement is included within the scope of this Self-Certification* |

# Assessment Guidance - Compliance

## R1

* + - 1. To determine applicability to CIP-012-1:
				1. Confirm what Control Center(s)[[1]](#footnote-2) were identified, including those owned or operated by different Responsible Entities.
				2. Is Real-time Assessment or Real-time monitoring data transmitted between any applicable Control Center(s)?

|  |
| --- |
| Entity Narrative  |
| Response: (a)(b) |

* + - 1. Provide evidence of the documented specification for data necessary to perform Real-time Assessments and Real-time monitoring, for example IRO-010 and/or TOP-003.

|  |
| --- |
| Evidence of CIP-012 Data Specification |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide each documented plan that addresses the applicable requirement parts in CIP-012 R1. Please identify where the plan addresses:
				1. Mitigation of risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
				2. Security protection(s) used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
				3. Applying security protection(s) for transmitting Real-time Assessment and Real-time monitoring data between any applicable Control Centers.
				4. Responsibilities of each entity for applying security protection(s) to Real-time Assessment and Real-time monitoring data transmissions, if applicable.

|  |
| --- |
| Evidence of Documented Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. For each Control Center[[2]](#footnote-3), for Real-time Assessment and Real-time monitoring data being transmitted between Control Centers, provide the following evidence:
				1. Implementation of security protection(s) used to mitigate the risks posed by unauthorized disclosure and unauthorized modification;
				2. Identification of where security protection(s) are applied for transmitting; and
				3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection(s) to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

|  |
| --- |
| Evidence of Security Protections  |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Pursuant to CIP-012-1 R1, please provide a list of any CIP Exceptional Circumstances (CEC) to this requirement and include the beginning date of the CEC, ending date of the CEC, Control Center(s) affected, and a description of the situation which triggered the CEC.

|  |
| --- |
| CIP Exceptional Circumstances |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Assessment Guidance - Controls

**Controls Instructions:**

In this section of the document, WECC asks you to identify/describe the controls your entity put in place to mitigate the risk(s) addressed by this Standard. When WECC asks you to "provide associated evidence," you should provide any evidence (examples include checklists, processes, procedures, training, sign-in sheets, *etc*.) demonstrating your entity *created* a control and *implemented* the control.

If you have any questions, please reach out to internalcontrols@wecc.org.

**Controls Questions:**

1. How does your entity verify it correctly identifies Real-time Assessment and Real-time monitoring data transmitted between Control Centers?
	1. Does this include data requests that do not indicate which data is Real-time Assessment and Real-time monitoring data?

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. How does your entity confirm protections mitigate the risks to data confidentiality and integrity? If your entity also has protections to mitigate risk to availability, please include these as well.
	1. How does your entity identify the risks posed by the communication channels transmitting Real-time Assessment and Real-time monitoring data between Control Centers?
	2. How does your entity evaluate the risks when a demarcation point[[3]](#footnote-4) is not in a Control Center owned or operated by you?
	3. How does your entity evaluate the risks to the physical security of assets where protections are applied?
	4. If your entity uses any additional layered security controls that are not documented elsewhere, please list them below.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. How does your entity verify the effectiveness of implemented protection methods?
	1. How frequently are security measures reviewed for effectiveness?
	2. Does your entity use continuous monitoring methods?
	3. How does your entity verify the implementation and effectiveness of end-to-end security protections when Control Centers are owned or operated by different Responsible Entities?

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Evidence Submittal

Please submit the following evidence with the Guided Self-Certification response to the Secure Evidence Locker (SEL):

|  |  |
| --- | --- |
| CIP-012-1 Requirement | Evidence |
|  | This completed worksheet |
| **R1** | *Requirement is included within the scope of this SC:*CIP-012 Data SpecificationDocumented Plan(s)Security ProtectionsCIP Exceptional Circumstances |
| **As Applicable** | Controls Evidence (if provided in response to any *Assessment Guidance – Controls* questions) |

# Revision Table

|  |  |
| --- | --- |
| Revision Date | Description of Revision |
| Mm/dd/2023 | Initial version of CIP-012-1 Guided Self-Certification Worksheet |

1. Per the [NERC Glossary of Terms](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf), a Control Center is defined as, “*One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time 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.*” [↑](#footnote-ref-2)
2. If needed, select a random sample of Control Centers. Refer to Instructions (4) for guidance. [↑](#footnote-ref-3)
3. Additional guidance on demarcation points can be reviewed in the ERO Enterprise Endorsed CIP-012-1 Implementation Guidance. ([link](https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-012-1%20Communications%20Between%20Control%20Centers%20%282016-02%20SDT%29.pdf)) [↑](#footnote-ref-4)