**[Registered Entity Name]**

**NERC ID: [NCRXXXXX]**

**CIP-012-1 – Cyber Security –**

**Communications between Control Centers, R1**

**2nd Quarter 2024 Self-Certification**

# Instructions

1. Populate the cover page by adding your entity’s name and NERC Identification NCR number.
2. Download CIP-012-1from NERC’s website (if desired): <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-012-1.pdf>
3. Complete the steps listed for each Reliability Standard Requirement listed under **Assessment Guidance.**
4. Log into **Align** and complete your self-certification response (see Section [9.0 Self-Certifications](https://training.nerc.net/Home/ViewApplicationVideos?system=Align&role=Registered%20Entities)).
5. Submit via the ERO Secure Evidence Locker (ERO SEL) Site:
   1. This completed Worksheet (please do not rename).
   2. Specific evidence requested within this document. Please make sure to do the following:
      1. Use unique file names for each evidence file submitted (whenever possible, provide searchable .pdf or Word files).
      2. Identify which specific evidence files support each response made. (Please ensure file names and extensions in the Worksheet match what is submitted). These references and the use of unique file names help facilitate and expedite MRO’s review of the Self-Certification work that has been performed.
      3. Include internal control information related to the Reliability Standard and Requirement(s) in scope with supporting documentation of design and implementation of the internal control(s).

# Scope

The scope for this Self-Certification is **CIP-012-1 R1, Cyber Security – Communications between Control Centers**. Each Responsible Entity shall include the data from the monitoring period between **July 1, 2022 – January 31, 2024,** as applicable for each step in the Assessment Guidance below.

# Purpose:

To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

# Assessment Guidance

**R1 –**

1. **Determine your entity’s applicability to CIP-012-1 -** List Control Center(s)[[1]](#footnote-1), including those owned or operated by different responsible entities and indicate if Real-time Assessment or Real-time monitoring data is transmitted between it and any applicable Control Center(s).

|  |  |  |  |
| --- | --- | --- | --- |
| **Applicability of CIP-012-1** | | | |
| **Sending Control Center**  **(including associated data centers)** | **Is Real-time or Real-time monitoring data transmitted between it and any applicable Control Center?**  **Yes = CIP-012-1 is applicable. List Receiving Control Center in next column.**  **or**  **No = CIP-012-1 is not applicable.** | **Receiving Control Center** | **Indicate if the data between the Sending and Receiving Control Centers is -**  **one-way**  **or**  **two-way** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* + - 1. 2. **Data Specification -** Provide evidence of the documented specification for data necessary to perform Real-time Assessments and Real-time monitoring, per IRO-010 and/or TOP-003 or corresponding equivalent. IRO-010 and/or TOP-003 are included based on the intent provided by the SDT.

|  |  |  |
| --- | --- | --- |
| Evidence of CIP-012-1 Data Specification | | |
| File Name(s) | Relevant Page(s) or Section(s) | Comments |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* + - 1. 3. **Documented Plan(s) -** Provide each documented plan that addresses the applicable requirement parts in CIP-012-1 R1. Please identify where the plan addresses:

**R1 -** 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.

**R1.1 -** 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.

**R1.2 -** Applying security protection(s) for transmitting Real-time Assessment and Real-time monitoring data between any applicable Control Centers.

**R1.3 -** 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) | | | |
| Part | File Name(s) | Relevant Page(s) and/or Section(s) | Comments |
| R1 |  |  |  |
| R1.1 |  |  |  |
| R1.2 |  |  |  |
| R1.3 |  |  |  |

* + - 1. 4. **Implementation of Security Protections -** For each applicable Control Center listed in **question #1**, for Real-time monitoring data being transmitted between Control Centers, provide the following evidence:

**R1.1 -** Implementation of security protection(s) used to mitigate the risks posed by unauthorized disclosure and unauthorized modification;

**R1.2 -** Identification of where security protection(s) are applied for transmitting; and

**R1.3 -** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Evidence of Security Protections | | | |
| Control Center | Part R1.1 **File Name with relevant Page(s) or Section(s)** | R1.2 **File Name with relevant Page(s) or Section(s)** | R1.3 **File Name with relevant Page(s) or Section(s)** | Comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **CIP Exceptional Circumstances (CEC) -** Pursuant to CIP-012-1 R1, please list any CEC for CIP-012-1, including the start and end date, Control Center(s) affected, and a description of the situation that triggered it.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIP Exceptional Circumstances | | | | |
| CEC | Start Date | End Date | Control Center(s) affected | Description of the situation that triggered the CEC |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Internal Controls**

**Provide Internal Controls CIP-012-1**

The internal control options provided below are meant to allow Registered Entities to choose their best approach to provide their internal control information and are not limited by the monitoring period. **Please provide information for Internal Controls Option 1 or Option 2:**

* **Option 1** is to allow Registered Entities to provide their information as they see applicable and in their desired format.
* **Option 2** is to assist registered entities with specific questions on best practices for CIP-012-1 - R1.

***Internal Controls Option 1:***

Provide information that shows:

1. Internal controls incorporation into global program for CIP-012-1 - R1
2. Internal controls design (process, procedures, etc.)
3. Internal controls implementation/operational evidence (control tests or evidence showing execution of the internal controls indicated)

**Please indicate in this table:**

|  |  |
| --- | --- |
| **All Internal Control(s) related to CIP-012-1- R1** | |
| **Global Program Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Design Filename(s)** |  |
| **Comments** |  |
| **Internal Controls Implementation and/or Operational Evidence Filename(s)** |  |
| **Comments** |  |

***Internal Controls Option 2:***

The following questions may be used as an optional approach to address internal controls for **CIP-012-1 R1.**

*Note: These questions are like those used by MRO in audit engagements. If a process or the implementation is not documented, provide comments of internal control(s), and indicate “not applicable” in supporting evidence fields.*

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

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

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?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. How does your entity evaluate the risks when a demarcation point[[2]](#footnote-2) is not in a Control Center owned or operated by you?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. How does your entity evaluate the risks to the physical security of assets where protections are applied?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. If your entity uses any additional layered security controls that are not documented elsewhere, please list them below.

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

1. How does your entity verify the effectiveness of implemented protection methods?
   1. How frequently are security measures reviewed for effectiveness?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. Does your entity use continuous monitoring methods?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

* 1. 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 or other third parties?

|  |  |
| --- | --- |
| **Comments** |  |
| **Supporting Evidence Filename(s)** |  |

**Provide Assessment of R1**

Was each question shown to follow the appropriate procedure/process in accordance with NERC Reliability Standard CIP-012-1 R1?

Yes, respond “Compliant” for R1 to the Self-Certification in Align. Include a comment summary and upload supporting documentation to the ERO SEL.

No, respond “Not Compliant” for R1 to the Self-Certification in Align. Include a comment summary based on potential issues and upload supporting documentation to the ERO SEL.

Do not own, respond “Do Not Own” for R1 to the Self-Certification in Align. Include comments supporting the “Do Not Own” response and upload supporting documentation to the ERO SEL.

Do not meet the applicability requirements of the full Standard, respond “Not Applicable” for R1 to the Self-Certification in Align. Include comments supporting the “Not Applicable” response and upload supporting documentation to the ERO SEL.

*This response should not be used if the circumstance within the standard or requirement language did not happen. This response should only be used if the requirement or standard is not applicable at all to the entity (such as not registered for the function).*

# Document Submittals

MRO requires copies of the following be submitted with the Self-Certification response:

1. This worksheet;
2. Supporting documentation referenced in the Assessment Guidance; and
3. Evidence supporting the Internal Control Option 1 or Option 2 for each requirement.

Please make sure to use unique file names for each evidence file submitted and identify within your responses to the steps above which specific evidence files support each response. These references and the use of unique file names help facilitate and expedite MRO’s review of the Self-Certification work that has been performed.

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-1)
2. 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(2016-02%20SDT).pdf)) [↑](#footnote-ref-2)