

**Reliability Standard Audit Worksheet[[1]](#footnote-1)**

# CIP-012-2 – Cyber Security – Communications between Control Centers

***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]](#footnote-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 |  |  |

**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 |

Findings

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Req.** | **Finding** | **Summary and Documentation** | **Functions Monitored** |
| **R1** |  |  |  |

|  |  |
| --- | --- |
| **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.** The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability, of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

**1.1.** Identification of method(s) used to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;

**1.2.** Identification of method(s) used to mitigate the risk(s) posed by the loss of the ability to communicate Real-time Assessment and Real-time monitoring data between Control Centers;

**1.3.** Identification of method(s) used to initiate the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;

**1.**4. Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2; and

**1.5.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for implementing method(s) as required in Parts 1.1, 1.2, and 1.3.

**M1.** Examples of evidence may include, but are not limited to, documented plan(s) that meet the mitigation objective of Requirement R1 and documentation demonstrating the implementation of the plan(s). Examples of methods identified in the plan(s) may include, but are not limited to, one or more of the following for each Part:

Part 1.1

* Methods of mitigation used to protect against the unauthorized disclosure and unauthorized modification of the data (e.g., data masking, encryption/decryption) while such data is being transmitted between Control Centers
* Physical access restrictions to unencrypted portions of the network

Part 1.2

* Identification of alternative communication paths of methods between Control Centers
* Procedures explaining the use of alternative systems or methods for providing for the availability of the data
* Service level agreements with carriers containing high availability provisions
* Availability or uptime reports for equipment supporting the transmission of Real-time Assessment and Real-time monitoring data

Part 1.3

* Contract, memorandum of understanding, meeting minutes, agreement or other information outlining the methods used for recovery
* Methods for the recovery of links such as standard operating procedures, applicable sections of CIP-009 recovery plan(s), or similar technical recovery plans
* Documentation of the process to restore assets and systems that provide communications
* Process or procedure to contact a communications link vendor to initiate and or verify restoration of service

Part 1.4

* Descriptions or logical diagrams indicating where the implemented methods reside
* Identification of points within the infrastructure where the implemented methods reside
* Third party Agreements detailing where the methods are implemented if such methods are implemented by the third party

Part 1.5

* Contract, memorandum of understanding, meeting minutes, agreement, or other documentation outlining the responsibilities of each entity

**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-012-2 R2

***This section to be completed by the Compliance Enforcement Authority***

|  |  |
| --- | --- |
|  | [R1] Verify the Responsible Entity has identified any applicable Control Centers. |
|  | [R1] Verify the Responsible Entity has identified the transmission of Real-time Assessment and Real-time monitoring data between any applicable Control Centers. |
|  | [R1] Verify the Responsible Entity has documented one or more plans to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability, of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. |
|  | [R1 Part 1.1] Verify the documented plan(s) includes identification of method(s) used to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. |
|  | [R1 Part 1.2] Verify the documented plan(s) includes identification of method(s) used to mitigate the risk(s) posed by the loss of the ability to communicate Real-time Assessment and Real-time monitoring data between any applicable Control Centers. |
|  | [R1 Part 1.3] Verify the documented plan(s) includes identification of method(s) used to initiate the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. |
|  | [R1 Part 1.4] Verify the documented plan(s) includes identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2. |
|  | [R1 Part 1.5] Verify the documented plan(s) includes identification of the responsibilities of each Responsible Entity for implementing methods as required in Parts 1.1 through 1.3for any Control Centers owned or operated by different Responsible Entities. |
|  | [R1] Verify the entity has implemented, except under CIP Exceptional Circumstances, the documented plan(s) to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. |
|  | [R1] Verify the documented and implemented plan(s) achieves the security objective of the risk(s) posed by unauthorized disclosure, unauthorized modification, and loss of availability, of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. |
|  | [R1] If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to its applicable cyber security policies. |
| **Notes to Auditor:**   1. The Responsible Entity is not required to include oral communications in its plans. 2. See Applicability Section 4.2.3 for a description of Control Centers that are exempt from this Standard. 3. To mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers, the Responsible Entity may have a single comprehensive plan, a plan that references other individual plans, or individual plans for each sub-requirement. | |

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-2 may be found on the NERC web site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “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 because 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 in Docket No. RD24-3-000 “… CIP-012-2 improves upon and expands the protections required by Reliability Standard CIP-012-1 by requiring responsible entities to mitigate the risk posed by loss of availability of communication links and Real-time Assessment and Real-time monitoring data transmitted between Control Centers.”[[3]](#footnote-3)

Selected Glossary Terms

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

Control Center

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.

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to load; generation output levels; known Protection System and Remedial Action Scheme status or degradation, functions, and limitations; Transmission outages; generator outages; Interchange; Facility Ratings; and identified phase angle and equipment limitations. (Realtime Assessment may be provided through internal systems or through third-party services.)

Revision History for RSAW

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Reviewers** | **Revision Description** |
| 1 | 10/18/2024 |  | Initial Draft |
|  |  |  |  |
|  |  |  |  |

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 RSAW may provide 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 reserve the right to request from the Registered Entity additional evidence 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. [↑](#footnote-ref-1)
2. Compliance Assessment Date(s): The date(s) the compliance assessment (on-site audit, off-site spot check, etc.) occurs. [↑](#footnote-ref-2)
3. *Order Approving Reliability Standard CIP-012-2*, 187 FERC ¶ 61,086 at P9 (2024). [↑](#footnote-ref-3)