# A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-2
3. **Purpose:** To protect the confidentiality, integrity, and availability of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
4. **Applicability:**
   - **4.1. Functional Entities:** The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.
     - **4.1.1. Balancing Authority**
     - **4.1.2. Generator Operator**
     - **4.1.3. Generator Owner**
     - **4.1.4. Reliability Coordinator**
     - **4.1.5. Transmission Operator**
     - **4.1.6. Transmission Owner**
   - **4.2. Exemptions:** The following are exempt from Reliability Standard CIP-012-2:
     - **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
     - **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
     - **4.2.3.** A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.
5. **Effective Date:** See Implementation Plan for CIP-012-2.

# B. Requirements and Measures

**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]*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;

**1.1.** 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 or 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

# C. Compliance

## 1. Compliance Monitoring Process

**1.1. Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

**1.2. Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

**1.3. Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

## Violation Severity Levels

| R # | Violation Severity Levels | | | |
|---|---|---|---|---|
| | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| **R1.** | N/A | The Responsible Entity documented its plan(s), but failed to include one of the applicable Parts of the plan as specified in Requirement R1. | The Responsible Entity documented its plan(s), but failed to include two of the applicable Parts of the plan as specified in Requirement R1. | The Responsible Entity failed to document its plan(s) for Requirement R1;<br>OR<br>The Responsible Entity failed to implement three or more Parts of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances. |

## D. Regional Variances

None.

## E. Associated Documents

- Implementation Plan.
- Technical Rationale for CIP-012-2.

## Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | | Respond to FERC Order No. 822 | New |
| 1 | August 16, 2018 | Adopted by NERC Board of Trustees | |
| 1 | January 23, 2020 | FERC Order issued approving CIP-012-1Docket No. RM18-20-000 | |
| 2 | December 12, 2023 | Adopted by NERC Board of Trustees | Revised under Project 2020-04 |
| 2 | May 23, 2024 | FERC Order issued approving CIP-012-2 Docket No. RD24-3-000 | |