

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-1
3. **Purpose:** To protect the confidentiality and integrity 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-012-1:
 - 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-012-1.

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 and unauthorized modification of Real-time Assessment and Real-time monitoring data while 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 security protection 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 Control Centers;
 - 1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
 - 1.3. 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.
- M1.** Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

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 plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part 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-012-1.

Implementation Guidance.

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-012-1. Docket No. RM18-20-000; | |
| 1 | February 17, 2020 | Effective Date | 7/1/2022 |