Alberta Reliability Standard
Cyber Security – Communications between Control Centres
CIP-012-AB-2

A. Introduction

1. Title: Cyber Security – Communications between Control Centres

2. Number: CIP-012-AB-2

3. Purpose: To protect the confidentiality, integrity, and availability of **real-time assessment** and real-time monitoring data transmitted between **control centres**.

4. Applicability:

4.1. Functional Entities: The requirements in this **reliability standard** apply to the following functional entities, referred to as "Responsible Entities," that own or operate a **control centre**:

4.1.1. the **ISO**;

4.1.2. the **operator** of a **generating unit**, **operator** of an **aggregated facility**, and **operator** of an **energy storage resource** that is part of the **bulk electric system**;

4.1.3. the **legal owner** of a **generating unit**, **legal owner** of an **aggregated facility**, and **legal owner** of an **energy storage resource** that is part of the **bulk electric system**;

4.1.4. [Intentionally left blank.]

4.1.5. the **operator** of a **transmission facility** that is part of the **bulk electric system**; and

4.1.6. the **legal owner** of a **transmission facility** that is part of the **bulk electric system**.

4.2. Exemptions: The following are exempt from this **reliability standard**:

4.2.1. **Cyber assets** at facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2. [Intentionally left blank.]

4.2.3. A **control centre** that transmits to another **control centre 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 centre**.

5. Effective Date: The later of (i) July 1, 2029, and (ii) the first **day** of the first calendar quarter 24 months following **Commission** approval.

B. Requirements and Measures

R1. The Responsible Entity must 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 centres**. The Responsible Entity is not required to include oral communications in its plan. The plan must include: *[Alberta Risk Rating: 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 centres**;

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 centres**;

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 centres**;

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

1.5. If the **control centres** 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 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 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 centres.**
- Physical access restrictions to unencrypted portions of the network.

Part 1.2

- Identification of alternative communication paths or methods between **control centres.**
- 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-AB-5 recovery plan(s), and any amendments made thereto from time to time, 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

[Intentionally left blank.]

D. Regional Variances

None.

E. Associated Documents

- NERC Cyber Security – Communications between Control Centers Technical Rationale and Justification for Reliability Standard CIP-012-2
- AESO Information Document #2021-007, *Cyber Security - Communication between Control Centres* and any amendments made thereto from time to time

Alberta Reliability Standard
Cyber Security – Communications between Control Centres
CIP-012-AB-2

Version History

Version	Effective Date	Description of Changes
AB-2	The later of (i) July 1, 2029, and (ii) the first **day** of the first calendar quarter 24 months following **Commission** approval.	Revised based on NERC CIP-012-2 approved by FERC in docket No. 866. The revision improves upon and expands the protections required 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 centres. Two new parts are added to Requirement R1 to address availability: Part 1.2, which requires protections for the availability of data in transit; and Part 1.3, which requires protections to initiate recovery of lost (i.e., unavailable) communication links. Administrative updates to standardize formatting and drafting style.
AB-1	2022-07-01	Initial Release.