# Alberta Reliability Standard
# Cyber Security – Communications between Control Centres
# CIP-012-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between **control centres**.

## 2. Applicability

This **reliability standard** applies to the following entities, referred to as "Responsible Entities":

(a) the **operator** of a **generating unit**;

(b) the **legal owner** of a **generating unit**;

(c) the **operator** of an **aggregated generating facility**;

(d) the **legal owner** of an **aggregated generating facility**;

(e) the **operator** of a **transmission facility**;

(f) the **legal owner** of a **transmission facility**; and

(g) the **ISO**,

that own or operate a **control centre**.

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

(a) **cyber assets** at facilities regulated by the Canadian Nuclear Safety Commission; and

(b) a **control centre** that transmits to another **control centre** real-time assessment or real-time monitoring data pertaining only to the generating resource, transmission station, or substation co-located with the transmitting **control centre**.

## 3. Requirements

**R1** Each Responsible Entity must implement, except under **CIP exceptional circumstances**, one or more documented plans 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 centres**. The Responsible Entity is not required to include oral communications in its plan. The plan must include:

**R1.1** 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 centres**;

**R1.2** identification of where the Responsible Entity applied security protection for transmitting real-time assessment and real-time monitoring data between **control centres**; and

**R1.3** if the **control centres** 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 centres**.

## 4. Measures

The following measures correspond to the requirements identified in section 3 of this **reliability standard**. For example, MR1 is the measure for requirement R1.

**MR1** Evidence of implementing one or more documented plans and including the required elements of the plan as required in requirement R1 exists. Evidence may include documentation demonstrating the implementation of the plan and a documented plan, or other equivalent evidence.

## 5. Appendices

Appendix 1 – *Implementation Plan*

## Revision History

| Date | Description |
|---|---|
| 2022-07-01 | Initial release. |

## Appendix 1 – Implementation Plan

### 1. Purpose

The purpose of this appendix is to set the effective dates and the implementation timelines for **reliability standard** CIP-012-AB-1, *Cyber Security – Communications between Control Centres* ("CIP-012-AB-1").

### 2. Compliance with Reliability Standards

The Responsible Entities identified in section 2 of this **reliability standard** must comply with the requirements of CIP-012-AB-1 in accordance with the implementation schedule.

### 3. Effective Date

CIP-012-AB-1 will become effective on July 1, 2022. Responsible Entities must follow the phased implementation plan set out in sections 4 and 5 below.

### 4. Implementation Plan for the ISO

(a) Where the **ISO** has communications with a **control centre** external to Alberta the **ISO** must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2022.

(b) Where the **ISO** has communications with a **control centre** internal to Alberta the **ISO** must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2023.

### 5. Implementation Plan for all Responsible Entities, Excluding the ISO

All Responsible Entities listed in section 2 of this **reliability standard**, excluding the **ISO**, must be compliant with requirement R1 of CIP-012-AB-1 on July 1, 2023.