NERC CIP-012-1	CIP-012-AB-1	AESO Reason for Differences
Purpose To protect the confidentiality and integrity of Real time Assessment and Real time monitoring data transmitted between Control Centers	**1. Purpose** To protect the confidentiality and integrity of real time assessment and real time monitoring data transmitted between **control centres**.	
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.	**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**.	
Effective Date See Implementation Plan for CIP-012-1	**Effective Date** Refer to the implementation plan in Appendix 1.	
R1 The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to	**R1** Each Responsible Entity must implement, except under **CIP exceptional circumstances**, one or more documented plans to	

NERC CIP-012-1	CIP-012-AB-1	AESO Reason for Differences
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.	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 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**.	
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).	**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.	

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.