Reliability Standard Audit Worksheet

CIP-012-AB-1

CIP-012 Cyber Security - Communications between Control Centres

Standard Effective Date: July 1, 2022

Audit Summary

Registered Entity:	[Registered Entity name as it appears in the AESO ARS Registry]
Functional Entity:	[Functional entities for which the Registered Entity above was registered throughout the audit period]
Audit Period:	From: [Audit start date or standard effective date, whichever comes later] To: [Audit end date or standard withdrawal/supersede date, whichever comes first]
Audit:	[Scheduled (YYYY-QX) or Spot Check YYYY-MM-DD]
Compliance Monitoring Entity:	Alberta Electric System Operator (AESO)
Suspected Non-Compliance to the standard?	☐ **No** ☐ **Yes** [If **Yes**, list the requirements with suspected contravention findings e.g. R1, R2, R5]
Date of Completion	[Use YYYY-MM-DD format]

Assessment Commentary

[Information (if any) relevant to audit findings below]

Findings

R1 [Summary of Findings]

Alberta Electric System Operator
Calgary Place, 2500, 330-5th Avenue SW Calgary, AB T2P 0L4
Phone: 403-539-2450 | Fax: 403-539-2949
www.aeso.ca
@theaeso

CIP-012-AB-1

Cyber Security – Communications between Control Centres

Contact Information

Audited Entity	
Compliance Primary	Name: Title: Phone: Email:
Subject Matter Expert	Name: Title: Phone: Email:

AESO Team	
Lead Auditor	Name: Title: Phone: Email:
Auditor	Name: Title: Phone: Email:
Compliance Manager	Name: Title: Phone: Email:
Standard Owner	Name: Title: Phone: Email:

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**.

CIP-012-AB-1

Cyber Security – Communications between Control Centres

Compliance Assessment

Requirement and Measure	Evidence Submission	Evidence Description	Evidence	Assessment Approach	Auditor Notes
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**. **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.	**AR1** Please provide: (i) Dated documented plan(s) in accordance to R1; (ii) List of CIP exceptional circumstances; if there were no CIP exceltional circumstance during the audit period, an attestation letter to that effect.	Provide descriptions for AR1 (i) submitted evidence:	Embed file or link to evidence	Verify the Responsible Entity has identified any applicable **control centres**. Verify the Responsible Entity has identified the transmission of real-time assessment and real-time monitoring data between any applicable **control centers**. Verify the Responsible Entity has documented one or more 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 centers**. Verify the documented plan(s) includes 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 any applicable **control centers.** Verify the documented plan(s) includes identification of where the Responsible Entity applied security protection for transmitting real-time assessment and real-time monitoring data between any applicable **control centers**. If real-time assessment or real-time monitoring data is transmitted between any applicable **control centers** owned or operated by different Responsible Entities, verify the documented plan(s) includes identification of the responsibilities of each Responsible Entity for applying security protection to these transmissions. Verify the Responsible Entity has implemented, except under **CIP exceptional circumstances**, the 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**.	*For AESO use only*

Requirement and Measure	Evidence Submission	Evidence Description	Evidence	Assessment Approach	Auditor Notes
				Verify the documented and implemented plan(s) achieves the security objective of mitigating 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.** If the Responsible Entity has declared and responded to **CIP exceptional circumstances**, verify the Responsible Entity has adhered to its applicable cyber security policies.	
	or any other evidence to demonstrate compliance with R1.	Provide descriptions for other submitted evidence	Embed file or link to evidence		*For AESO use only*
Findings					
For AESO use only					

CIP-012-AB-1

Cyber Security – Communications between Control Centres

General Notes

The AESO developed this Reliability Standard Audit Worksheet (RSAW) to add clarity and consistency to the audit team's assessment of compliance with this reliability standard, including the approach elected to assess requirements.

Additionally, the RSAW provides a non-exclusive list of examples of the types of evidence a market participant may produce or may be asked to produce to demonstrate compliance with this reliability standard. A market participant's adherence to the examples contained within this RSAW does not constitute compliance with the reliability standard.

This document is not an AESO authoritative document and revisions to it may be made from time to time by the AESO. Market participants are notified of revisions through the stakeholder update process.

Notes to File

[For AESO use only: any observations, remarks or action items for future audits]

Revision History

Version	Issue Date	Description
Draft	Sept. 15, 2022	To be presented to TWG