CIP-012-AB-1 Implementation TWG September 2022 Discussion Summary

Session purpose and objectives

The purpose of the session is to engage stakeholders in discussions about the recently approved reliability standard CIP-012-AB-1, *Cyber Security - Communications between Control Centres* ("CIP-012-AB-1"). Specific session objectives include:

- Review the CIP-012-AB-1 requirements
- Present and seek feedback on:
  - AESO Information Document 2021-007, *Cyber Security – Communications between Control Centres* ("ID #2021-007"); and
  - the *CIP-012-AB-1 Reliability Standard Audit Worksheet* (RSAW).
- Share the AESO's key learnings on its implementation of CIP-012-AB-1
- Inform stakeholders about the AESO's proposed approach to CIP-012-AB-1 implementation for telecommunication links between each applicable Responsible Entity and the AESO's control centres
- Provide a forum for stakeholders and the AESO to engage in a discussion on CIP-012-AB-1 implementation, with the objective of assisting impacted stakeholders in meeting their CIP-012-AB-1 obligations by their effective date of July 1, 2023

Session agenda

- **Date: September 21, 2022**
- **Time: 9:00 a.m. to 12:00 p.m.**
- **Location: Virtual Teams Webinar**

Time	Agenda Item	Presenter
9:00 - 9:15	Welcome, Introductions, Housekeeping and Agenda	Kathryn Kuber
9: 15 - 9:30	Review CIP-012-AB-1	Visu Viswanathan
9:30 - 10:00	Discuss the AESO Information Document ID#2021-007 • Q&A	Visu Viswanathan
10:00 - 10:15	Share the AESO's Key Learnings on its CIP-012-AB-1 Implementation • Q&A	Haithem Al-Salam
10:15 - 10:30	Coffee break	
10:30 - 11:00	Discuss AESO *CIP-012-AB-1 Reliability Standard Audit Worksheet* • Q&A	Daniela Cismaru
11:00 - 11:30	Share AESO's Proposed Approach to CIP-012-AB-1 Implementation for Telecommunication Links. • Q&A	Visu Viswanathan
11:30 - 11:45	Next Steps and Session Close-Out	Visu Viswanathan Kathryn Kuber

CIP-012-AB-1 Implementation TWG September 2022 Discussion Summary

Attendees

Company
Alberta Electric System Operator {“AESO”)
AltaLink Management Ltd.
Ampere Industrial Security
ATCO Electric
BluEarth Renewables
Capital Power Corporatioin
City of Lethbridge
City of Medicine Hat
ENMAX Energy Corporation
ENMAX Power Corporation
EPCOR Distribution & Transmission Inc.
Lionstooth Energy Inc.
Market Surveillance Administrator
Neoen
Suncor Energy Inc.
TransAlta
WSP

Session highlights

Welcome and Introductions

- The AESO welcomed everyone, introduced speakers, and presented housekeeping items, the AESO’s Stakeholder Framework, and gave an overview of the agenda.
- The new standard CIP-012-AB-1 has been in effect for AESO since July 1, 2022 and takes effect for stakeholders as of July 1, 2023.

Reliability Standard CIP-012-AB-1, Cyber Security - Communications between Control Centres (“CIP-012-AB-1”) and draft AESO Information Document ID#2021-007, Cyber Security - Communications between Control Centres (“ID#2021-007”)

- The AESO presented slides on the approved CIP-012-AB-1 reliability standard, including the purpose, applicability, exemptions, and requirements.
- The AESO gave an overview of the content of ID#2021-007 and highlighted the following items, which are found in the slides:
    - NERC CIP-012 guidance material

- The meaning of real-time assessment and monitoring data
- Applicable and out-of-scope communication links,
- Identification of types of security protection and recommendations related to physical and logical protection, including the AESO's recommendation, for logical protection, to use a minimal encryption level IPSEC VPN Tunnel, for applicable communication links between AESO and applicable control centres; and suggestion that encryption can be implemented at the 1st device inside an entities own network, so the protection is within the entity's control.
- The responsibilities of each entities' responsibilities and a recommendation that entities exchange documentation to outline each entities' responsibilities.
- Guidance on the steps to follow when developing a plan, including identifying applicable data and communication links, the protection methods.

Share the AESO's Key Leanings on its CIP-012-AB-1 Implementation

- The AESO presented slides on its key learnings from its own implementation of CIP-012-AB-1.

Discuss AESO CIP-012-AB-1 Reliability Standard Audit Worksheet

- The AESO presented and walked attendees through its draft CIP-012-AB-1 RSAW.
  - The AESO noted that it starts with an assessment of whether the requirement is applicable to a Responsible Entity.
  - The Compliance Assessment – how we measure compliance and the evidence to be submitted to demonstrate compliance to the requirement
  - Assessment Approach – outlines the questions and evidence the AESO will verify during their audit of your compliance
- The AESO noted that when the compliance team is evaluating a market participants compliance, it utilizes the ID and NERC guidance, including the definitions and examples provided.
- The AESO also shared that with the ARS Enhancements Initiative one of AESO's commitments is to share information and documents as early in the process as available.
- The AESO clarified the intent of the RSAW is for AESO to communicate and provide guidance to market participants around how to demonstrate compliance, not specifically on how to be compliant but how to demonstrate compliance, for each requirement.
- The AESO indicated that the draft RSAW does not currently include the evidence submission. This will be coming once the type of evidence to show implementation has been determined after the ID is finalized. However, the draft ID provides guidance on how Responsible Entities can implement the plan.
- The draft is available for participants to review and provide feedback.

Share AESO's Proposed Approach to CIP-012-AB-1 Implementation for Telecommunication Links

- The AESO presented its proposed approach to CIP-012-AB-1 implementation on applicable communication links between the AESO and Responsible Entities.

Next Steps and Close Out

- The AESO went through the next steps and key dates that were included in the presentation. Highlighting the fact that the AESO has started initiating one-on-one detailed technical discussion between the AESO and applicable entities' network and SCADA teams to assess capabilities and timeline for technical implementation of CIP-012-AB-1 for each applicable communication link.
- The AESO thanked all attendees for coming and participating in the session and asked stakeholders to answer survey questions prior to leaving the session.

Attendee Questions and AESO Responses from the Session

- During the session, the following questions were asked by attendees and responses were provide by the AESO:
    - Question: Please confirm that an owner of a generating unit (GFO) control centre is only in scope if the GFO control centre is aggregating the real-time data from multiple generating resources and forwarding them to the AESO?
        - AESO Response: The communication link between a GFO control centre to a generating resource is out of scope, however, communication from GFO control centre to the AESO is in scope.
    - Question: For the generation unit in an industrial complex, the generator data is sent to the AESO through the communication link between an operator of a transmission facility (TFO) control centre to the AESO. Will the communication link between the generation unit and the transmission control centre be in scope or out of scope? Can you update the drawings to reflect your answer?
        - Response: The communication link between the GFO Resource Control Room and the TFO control centre would be out of scope in such situation. The AESO can update Figure 1 to reflect this situation.
        - Action: The AESO will update Figure 1 to include a situation where a generating resource has a communication link with a TFO control centre, which in turn communicates with the AESO control centre.
    - Question: Can AESO comment on the scope of the term "fulfilling duties" in the definition of "real time monitoring". For example, would a P&C technician remotely connecting to a transmission substation HMI to view a setting or real value for the purposes of validating values sent to control centre operators be fulfilling duties?" My interpretation would be that it would not include that but wanted to validate.
        - AESO Response: It means to fulfil the AESO and market participant duties related to the real-time assessment and real-time data only.
    - Question: Can the AESO confirm the market portal, including the ADAMS dispatch system, is out of scope of CIP-012-AB-1?
        - AESO Response: The Focus of CIP-012-AB-1 on control centre to control centre communication, so the market portal is out of scope.

- Question: If a market participant has more than one control centre which communicates internally between them, is that link in-scope for CIP-012-AB-1?
  - AESO Response: If a market participant has a primary and back-up control centres, like the AESO, then communication between the primary and back-up control centre are in-scope for CIP-012-AB-1.
- Question: For communication between TFO control centres, if there is no real-time assessment or monitoring data communication, is CIP-012 applicable to this communication link?
  - AESO Response: Should a communication link exist between TFO control centres for purposes other than communicating real-time monitoring and assessment data, then the communication link would be out of scope since no applicable data is being communicated.
- Question: Is Figure 3 in the NERC Rationale document, which is also referenced in section 5.4 of the draft ID # 2021-007, applicable for the determination of exemptions related to audit purposes? Are those exemptions in the NERC document sufficient to support an audit exemption.
  - AESO Response: The information in information documents posted by AESO are to support both the AESO and Responsible Entities. They are used by the compliance team for audit assessments. Where the information document clarifies which control centres are within scope, the audit team will be assessing for the applicable control centres in the same way.
- Question: The AESO ID specifically references Figures 1 to 3 of the NERC Rationale document but does not reference Figure 4. Can the AESO speak to this exclusion?
  - AESO Response: The AESO agrees with the information provided in Figure 4.
  - Action: The AESO will update the ID to include Figure 4 of the NERC Rationale document.
- Question: Given that the Reliability Coordinator's definition of real-time monitoring is critical to determining applicability - will the AESO entertain applicability requests on CIP-012 to assist entities in ensuring the standard has been applied correctly in advance of their next audit?
  - AESO Response: The AESO has put together the ID#2021-007 and is here to ensure market participants have a good understanding of the CIP-012 requirements to protect the overall integrity and cybersecurity protection of the grid. If following this session, the AESO's Request for Information (RFI) process can be used to request clarification of applicability. The AESO does not confirm applicability using the RFI process; however, we will respond to any clarifying questions that arise, so please include details around your challenges.
- Question: Is there any additional guidance that AESO can give between the distinction between a 'control room' vs a 'control centre'?
  - AESO Response: The AESO's Consolidated Authoritative Document Glossary (CADG) contains the definition of control centre. The AESO understands that this may not align with market participants use of the term control centre, and that

some entities internally use control room and control centre interchangeably. When you evaluate your control centre for use in the standards, entities should use the AESO's definition. The AESO also noted that control room is not defined in the AESO's CADG.

- Action: The AESO will look at referencing its 'control room' information, that is in the draft amended COM-001 ID (ID#2012-001RS, Communications) in ID#2021-007, to help clarify what the AESO means by control room.

- Question: Does an entity need to enable encryption if it has physical protection?
  - AESO Response: The Responsible Entity must assess what security protection is best for your scenario through its protection plan. An entity may decide physical protection is best for a particular communication link, but logical is best for other communication links. Both are sufficient.
- Question: For encrypted communications between control centres, can the encryption stop/restart at a junction point which is also protected physically by the entity? For example. Site A<>B encrypted. Site B1-B2 physically protected, site B2<>C encrypted. AESO to Point B and then exit through another router to Point C – does the whole line need to be protected.
  - AESO Response: Data must be protected for compliance and intent of the standard so we will not tell you how to protect but we will provide clarity, however the responsibility to protect is up to each entity. But yes, in the scenario given, it sounds like the intent of CIP-012 is being met.
- Question: If there was a private fiber connection between two control centres, can physical security be applied to the intermediate junction cabinets (housing terminations), or does it need to be applied to the entire path of the fiber?
  - AESO Response: All the data must be protected
- Question: for the ISD, the is the fiber network within the site footprint and fiber network connected externally outside the footprint. Will the fiber network within the site footprint be deemed as the private fiber connection?
  - AESO Response: A fiber is considered private when the entity has full control of the communication link and it is not open to others publicly.
- Question: Will the AESO support DNP3 encryption?
  - AESO Response: Yes, we have implemented DNP3 for other communications, but we want to focus on the protection, not the communication protocol.
- Question: Will the AESO determine PSK / Cert for encryption?
  - AESO Response. Yes; however, it is yet to be determined.
- Question: What is the role of telecommunication providers in the implementation? Also, any evidence to be gathered from telecoms for audit?
  - AESO Response: The AESO recommends implementing protection on a device within your network. If you do work with a service provider, you may need to collect configuration files or encryption implementation evidence from them depending on how the protection is implemented.