DRAFT Information Document #2021-007
Cyber Security - Communication between Control Centres

Information documents are not authoritative. Information documents are for information purposes only and are intended to provide guidance. In the event of any discrepancy between an information document and any authoritative document[1] in effect, the authoritative document governs.

1 Purpose

This information document relates to the following authoritative document:

- Reliability Standard CIP-012-AB-1, *Cyber Security - Communication between Control Centres* ("CIP-012-AB-1")

The purpose of this information document is to provide each Responsible Entity with clarity regarding the use of NERC guidance material in Alberta, the meaning of the terms real-time assessment and real-time monitoring data, and additional information to assist stakeholders with implementing CIP-012-AB-1.

2 NERC Guidance Documents for CIP-012-1

The following NERC CIP-012-1 documents provide useful guidance for each Responsible Entity:

- *Cyber Security – Communications Between Control Centers Implementation Guidance for CIP-012-1 March 2020 version,* ("NERC Implementation Document"); and
- *Cyber Security - Communications between Control Centers Technical Rationale and Justification for Reliability Standard CIP-012-1, August 2018 version* ("NERC Rationale Document").

The NERC CIP-012-1 documents are relevant in the Alberta context. However, there are some discrepancies between NERC and Alberta that each Responsible Entity should be mindful of when interpreting how to apply to this guidance to its Alberta facilities. These differences are described in the following subsections.

3 Real-time Assessment and Real-time Monitoring Data (section 1 of CIP-012-AB-1)

As set out in section 1 of CIP-012-AB-1, the purpose of CIP-012-AB-1 is to protect the confidentiality and integrity of real-time assessment and real-time monitoring data.

The NERC CIP-012-1 documents describe real-time assessment and real-time monitoring data, requiring protection under CIP-012-1, as a subset of data transmitted pursuant to NERC reliability standards TOP-003, *Planned Outage Coordination* ("NERC TOP-003") and IRO-010, *Reliability Coordinator Data Specification and Collection*.

The AESO determined that NERC TOP-003-3, *Operational Reliability Data* was not applicable in Alberta[2]. In addition, the latest version of the Alberta reliability standard IRO-010, which is IRO-010-AB-2, *Reliability Coordinator Data Specification and Collection* ("IRO-010-AB-2") is only applicable to the AESO. As a result of the differences between the referenced NERC and AESO reliability standards, the AESO has provided further clarity on real-time assessment and real-time monitoring data, as it relates to CIP-012-AB-1, in this section 3 of the information document.

In Alberta, the real-time assessment and real-time monitoring data referenced in CIP-012-AB-1 includes:

- Appendix 1 to 5 of Section 502.8 of the ISO rules, *SCADA Technical and Operating Requirements* ("Section 502.8")*;*
- Section 502.9 of the ISO rules, *Synchrophasor Measurement Unit Technical Requirements*

[1] "Authoritative document" is the general name given by the AESO to categories of documents made by the AESO under the authority of the *Electric Utilities Act* and associated regulations, and that contain binding legal requirements for either market participants or the AESO, or both. Authoritative documents include the ISO rules, the reliability standards, and the ISO tariff.

[2] TOP-003-3 is listed on the AESO's Non-applicable standards list found on the AESO website.

("Section 502.9"); and

- IRO-010-AB-2.

3.1 Real-time assessment meaning

The AESO considers the term "real-time assessment" to have a similar meaning as the NERC defined term "real-time assessment". Due to differences between the AESO and NERC defined terms and functional entity types, the term has a slightly different meaning in Alberta. The meaning of the term real-time assessment and examples are provided below. Note that AESO defined terms are bolded for added clarity and can be found in the AESO's *Consolidated Authoritative Document Glossary*.

> Real-time assessment means an evaluation of system conditions using real-time data to assess pre-**contingency** and potential post-**contingency** operating conditions. The assessment is expected to reflect applicable inputs including: load; **generating unit** and **aggregated generating facility** output levels; known **remedial action scheme** status or degradation, functions, and limitations; any outage of one or more **transmission facility**, any outage of one or more **generating unit** and **aggregated generating facility**; **interchange**; **facility ratings**; and identified phase angle and equipment limitations. Real-time assessment may be provided through internal systems or through third-party services.

3.2 Real-time assessment examples

Real-time assessment data is all data that is an input to or generated by a real-time assessment. Examples of this data include: load; generating unit and aggregated generating facility output levels, remedial action scheme status; transmission facility status; real power and reactive power flow; system voltage; and system frequency.

Appendix 1 to 5 of Section 502.8 of the ISO rules, *SCADA Technical and Operating Requirements* ("Section 502.8") outline the real-time data requirements for market participants. The real-time data outlined in Section 502.8 that are used in a real-time assessment or generated by a real-time assessment are considered real-time assessment data.

3.3 Real-time monitoring meaning

NERC does not have a definition for real-time monitoring. The AESO interprets "real-time monitoring" to mean the act of observing the current state of the interconnected electric system in real time by operating personnel to fulfill the AESO and each market participant duties.

The AESO considers any real-time data that is used by the AESO and by each market participant, for the real-time monitoring of its facility, to be real-time monitoring data. This data includes information that is provided through supervisory control and data acquisition ("SCADA") systems.

3.4 Real-time monitoring examples

Examples of real-time monitoring data include: load; generating unit and aggregated generating facility output levels; substation equipment status; real power and reactive power flow; system voltage; and system frequency.

All data identified in Appendix 1 to 5 of Section 502.8 that is received through real-time monitoring systems, including the energy management system ("EMS") and SCADA systems, is real-time monitoring data.

4 Responsible Entities (section 2 of CIP-012-AB-1)

When reviewing the NERC CIP-012-1 documents, keep in mind that, in the Alberta legislative and regulatory framework:

- the AESO performs the function of a NERC Reliability Coordinator ("RC") and Balancing Authority ("BA"); and
- the operator of a transmission facility performs the function of a NERC Transmission Operator

("TOP").

5 Control Centres (section 2 of CIP-012-AB-1)

5.1 CIP Impact Ratings

The Section 2 of CIP-012-AB-1 does not set out applicability by CIP impact levels, as are described in reliability standard CIP-002-AB-5.1, *BES Cyber System Categorization* ("CIP-002-AB-5.1"). As noted in the NERC guidance material, this means that CIP-012-AB-1 is applicable to all control centres categorized as low, medium, or high impact using the Impact Rating Criteria outlined in Attachment 1 of CIP-002-AB-5.1.

5.2 Owners and Operators of Electric Distribution Systems

CIP-012-AB-1 does not apply to an entity that is an owner or operator of an electric distribution system ("DFO"). Therefore, generally, a facility that, at all times, exclusively hosts operating personnel that monitors and controls an electric distribution system is out the scope of the CIP-012-AB-1 applicability.

However, in situations where the entity is also the owner or operator of a transmission facility, and the facility meets the AESO's definition of control centre, the facility would be in scope. For example, if the facility hosts operating personnel that monitors and controls in real-time to perform reliability tasks both an electric distribution system and part of the bulk electric system, it would be considered a control centre and CIP-012-AB-1 would be applicable.

5.3 Exemptions (Section 2 – exemption of CIP-012-AB-1)

Section 2 of CIP-012-AB-1 provides exemptions to CIP-012-AB-1 applicability.

The AESO supports the guidance provided in the NERC Rational Document on exemptions to NERC CIP-012-1 applicability. Section *CIP-012 Exemption (4.2.3) for certain Control Centers*[3] of the NERC Rationale Document provides guidance on how each Responsible Entity may assess the exemption criteria.

5.4 Generalized Assessment of Communication Link Applicability (Section 2 -applicability of CIP-012-AB-1)

Figures 1, 2, and 3[4] in the NERC Rationale Document, illustrate the applicability and exemptions for 3 different generating resource communication link configurations that provides a good reference for owners and operators of generation units and aggregated generating facilities ("GFO").

In the Alberta context, generally exemption (b) in Section 2 of CIP-012-AB-1 applies to communication links between:

(a) a control room for individual generating unit or aggregated generating facility; and

(b) a control room in a control centre for an operator of a transmission facility, an operator of a generating facility, or the AESO.

Figure 1 is provided to help illustrate the applicability and exemptions for communication links:

[3] Section *CIP-012 Exemption (4.2.3) for certain Control Centers* is found on PDF pages 4 to 8 of the NERC Rationale Document.
[4] Figures 1, 2, and 3 are found on PDF pages 5 to 7 in the NERC Rationale Document.

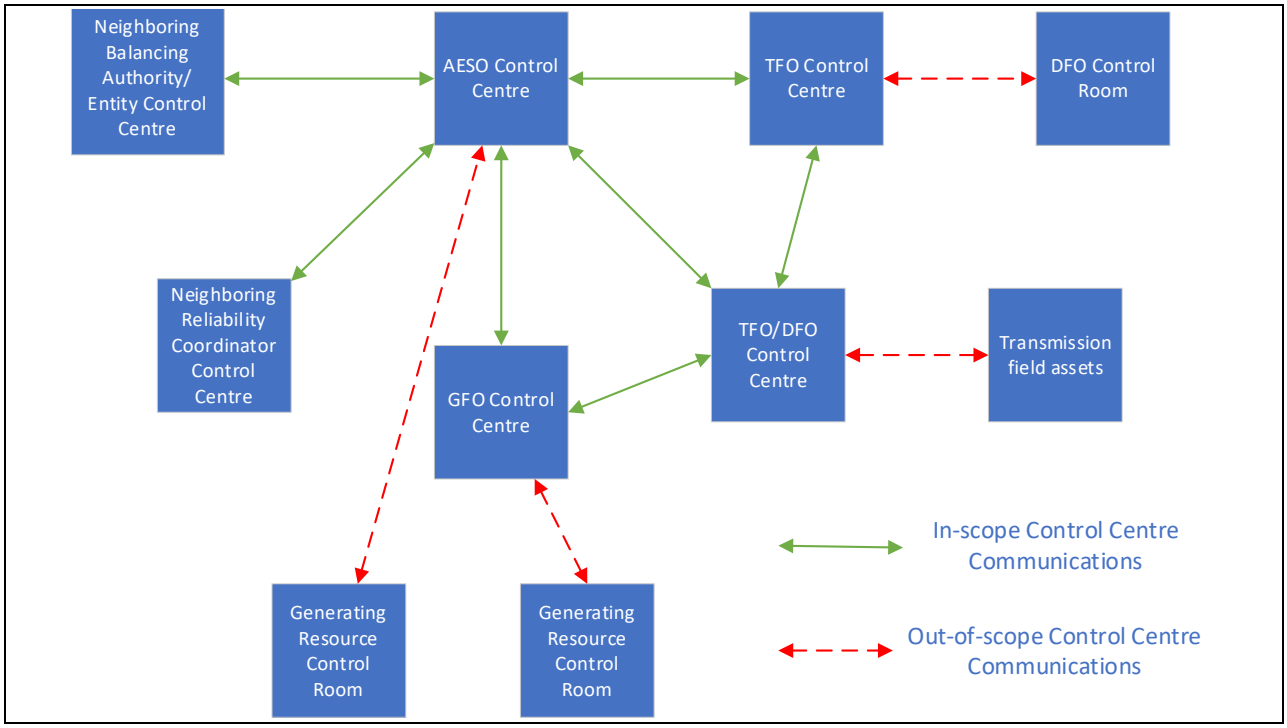

Figure 1: Reference model showing generalized applicability of control centre communication links

5.5 Primary and Backup Control Centres (section 2 of CIP-012-AB-1)

The NERC Implementation Document provides guidance on how NERC CIP-012- 1 applies to communication between a Responsible Entity's primary and backup control centres[5]. Specifically, Section *Identification of Where Security Protection is Applied by the Responsible Entity (R1.2)* and *Reference Model* of the NERC Implementation Document provides helpful guidance.

Figure 2 illustrates an Alberta-specific reference model to provide further guidance:

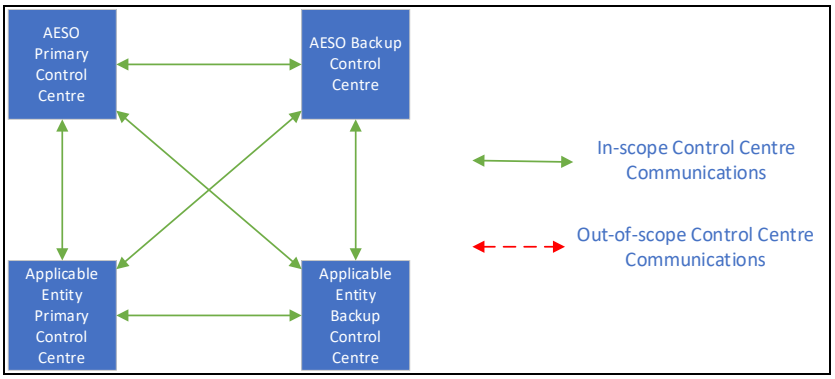

Figure 2: Reference model showing applicability of communication links between primary and backup control centres

6 Identification of Security Protection (section 3 (R1.1) of CIP-012-AB-1)

To meet Requirement R1.1 of CIP-012-AB-1, the applicable Responsible Entity is responsible for

[5] Section *Identification of Where Security Protection is Applied by the Responsible Entity (R1.2)* is found on PDF page 6, and the *Reference Model* section**,** is found on PDF page 8 and 9 of the NERC Implementation Document.

assessing and determining the feasible solution to protect each of its communication links. The AESO agrees with the guidance material provided in the NERC Implementation Document on the identification of security protection.

The NERC Implementation Document provides guidance on identifying the security protection an entity may choose for mitigating these risks. Specifically, the *Identification of Security Protection* section and *Reference Model* sections[6].

The security protection implemented by each Responsible Entity may be a combination of both physical protection and logical protection. A Responsible Entity may choose one type of security protection for a specific communication link, while another type of security protection is implemented for another communication link. The decision to implement a consistent or a variety of security protection is left to each Responsible Entity.

6.1 Scenarios where Physical Security Protection is appropriate

This section provides several scenarios for consideration by each Responsible Entity in its implementation of security protection to meet Requirement R1 of CIP-012-AB-1. In addition to the examples provided in this information document, the AESO agrees with the reference model examples provided in the NERC Implementation Document.

Figure 3 illustrates an example where 2 control centres are owned and operated by the same Responsible Entity and the technology used in the communication network/medium between the 2 control centres allows for physical protection.

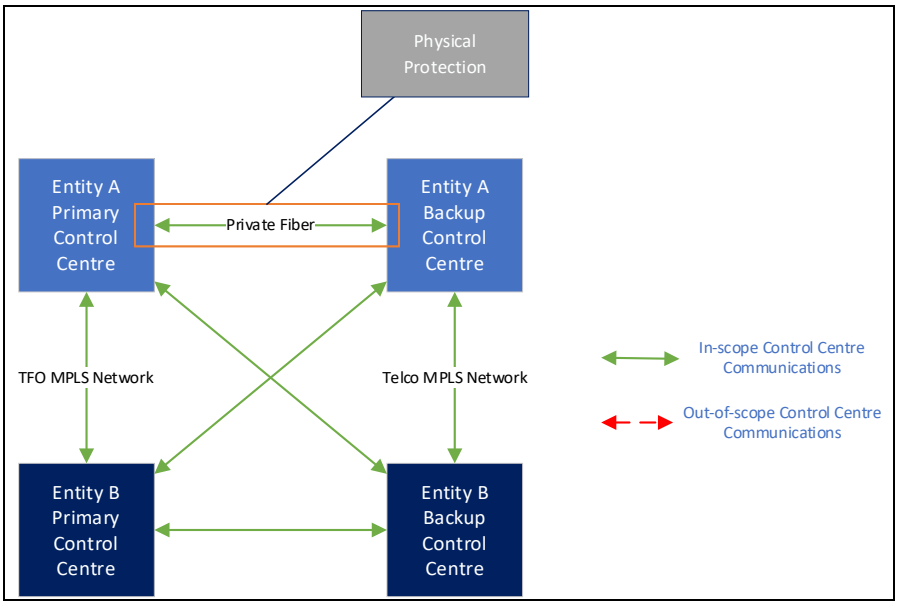

Figure 3 – Reference model showing physical protection between primary and backup control centres where applicable

Another scenario presented in the NERC Implementation Document under *Identification of Security Protection (R1.1)* section[7], is where 2 control centres, each owned and operated by separate Responsible Entities, are in close physical proximity such that physical protection may be appropriate. Figure 4 illustrates this scenario.

[6] The *Identification of Security Protection* section and *Reference Model* sections are found on PDF pages 5 and 6, and PDF page 9, respectively, of the NERC Implementation Document.
[7] *Identification of Security Protection (R1.1)* section is found on PDF page 5 of the NERC Implementation Document.

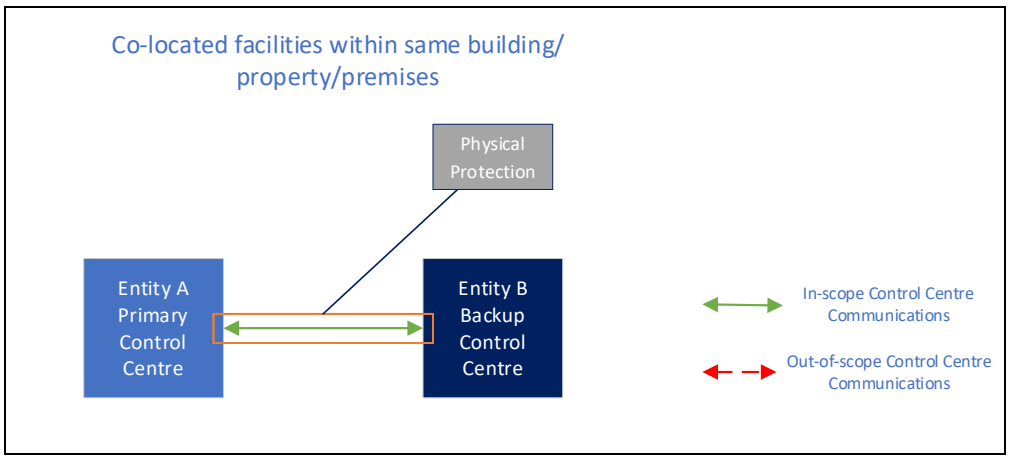

Figure 4 – Reference model showing Physical Protection between Entity A Primary Control Centre and Entity B Backup Control Centre where the two control centres are co-located within the same building/property/premises

6.2 Identification of AESO's Security Protection for applicable communication links

The AESO has telecommunication links with many applicable entities that are used for the exchange of real-time assessment and real-time monitoring data. These communication links are provisioned through the TELUS MPLS network, Utility Telecom Network ("TFO Telecom Network"), or an alternate service provider. The AESO proposes the adoption of IPSEC VPN Tunnels as security protection for the applicable communication links. The preferred method for the implementation of IPSEC VPN Tunnels is site-to-site connectivity using one or more encryption devices owned and managed by the Responsible Entities, meaning the AESO and each applicable entity.

The AESO expects each Responsible Entity to ensure that its encryption devices are: capable of Internet Key Exchange ("IKE") policy and IPsec policy configured to a defined minimum encryption level; and reside in a secured area within a control centre accessible only to designated personnel. The following shows the details of the minimum encryption level. The minimum encryption level is expected to change in the future as vulnerabilities, industry standards, hardware capabilities, and encryption technology develops. Figure 5 shows the AESO's expected IPsec VPN Tunnel minimum encryption levels.

IPSEC VPN Tunnel - IKE policy and IPsec policy minimum encryption level

Phase 1 IKE Parameters	
PSK/Cert:	TBD
IKE Mode:	IKEv2
Key Exchange Encryption:	AES-256
Data Integrity:	SHA-512
Diffie-Helman (DH) Group:	5 (1536-bit)
SA Timeout:	14400 seconds
Phase 2 IPSec Parameters	
PSK/Cert:	TBD
IKE Mode:	IKEv2
Data Encryption:	AES-256
Data Integrity:	SHA-512
PFS DH Group:	enabled Group 5 (1536-bit)
SA Timeout:	14400 seconds

Figure 5 – IPsec VPN Tunnel minimum encryption level

6.3 Standardized Security Protection (section 3 (R1.1) of CIP-012-AB-1)

Section 6.2 of this information document provides the standardized logical security protection the AESO will be implementing for applicable communication links. The AESO recommends entities consider the same security protection for applicable communication links between their control centre and another entity's control centre.

7 Identifying where an entity shall apply security protection (section 3 (R1.2) of CIP-012-AB-1)

The NERC Implementation Document, in Sections *Identification of Where Security Protection is Applied by the Responsible Entity (R1.2)* and *Reference Model*[8] respectively, provides guidance on identifying where security protection is applied by the applicable entity. The AESO agrees with the NERC guidance and agrees that the guidance is applicable in Alberta. In addition to the guidance provided in the NERC document, the AESO offers the following for consideration.

For logical security protection, the NERC Implementation Document provides guidance that the logical security protection can be applied at the WAN Router, which is sometimes referred to as the edge router.

Even though the WAN Router may be physically located within the Responsible Entity's control centre, Responsible Entities typically rely on the WAN service provider, i.e., a telecommunication service provider, to make changes or updates to the configurations of the WAN router, including enabling and configuration downloads of encryption settings.

Therefore, the AESO recommends entities consider applying logical security protection at a device that is fully accessible by the Responsible Entity's staff, i.e., at the first device inside their network after the edge WAN Router. This will allow for better management of the security protection being applied by the Responsible Entity.

[8] *Identification of Where Security Protection is Applied by the Responsible Entity (R1.2)* and *Reference Model sections are* found on PDF pages 6 and 10, respectively of the Implementation Document.

Figure 6 is provided to help illustrate this recommendation:

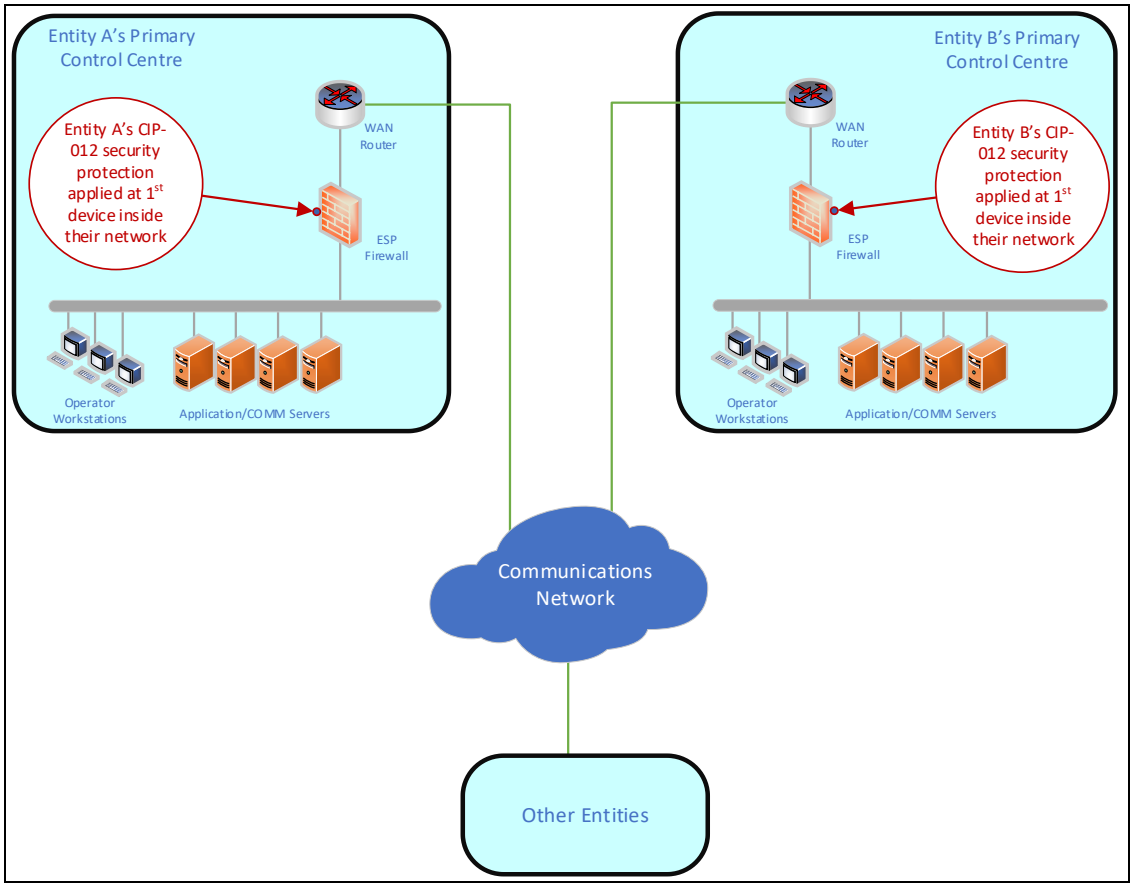

Figure 6 – Logical security protection location inside entity network after edge WAN routers

For Requirement R1.2 of CIP-012-AB-1, the AESO does not expect a Responsible Entity to identify where other Responsible Entities have applied the security protection for their applicable communication link. For any communication link between a Responsible Entity's primary and backup control centre, the AESO expects the Responsible Entity to identify the location of the security protection applied at both control centres.

8 Identifying Responsibilities when the control centres are owned or operated by different applicable entities (section 3 (R1.3) of CIP-012-AB-1)

The NERC Implementation Document, in Sections *Identification of Responsibilities when the control centers Owned or Operated by Different Responsible Entities (R1.3)* and *Reference Model*[9] provides guidance on identifying the responsibilities of applicable entities when the control centres are owned or operated by different entities. The AESO agrees with the guidance provided and that it is applicable in Alberta.

In addition to the NERC guidance provided, the AESO offers the following information. In the case of control centres owned or operated by different Responsible Entities, both Responsible Entities are expected to include each others' responsibilities in their plans to satisfy Requirement R1 and R1.3 of CIP-012-AB-1. The NERC Implementation Document suggests that entities may collect letters from each other

[9] Sections *Identification of Responsibilities when the control centers Owned or Operated by Different Responsible Entities (R1.3)* and *Reference Model* are found on PDF page 7 and 8, and PDF page 10, respectively, of the Implementation Document.

indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement, or manual indicating ownership or responsibility. The AESO suggests that a letter indicating an entity's ownership or responsibilities for a specific communication link as applicable to CIP-012-AB-1 be exchanged between entities. And each Responsible Entity is expected to include the other entity's responsibilities in their own plan. The letter from the other entity identifying their responsibilities can be included as supporting documentation.

For each Responsible Entity that has an applicable communication links with the AESO, the AESO expects to provide the Responsible Entity with a document that outlines the AESO's responsibilities with respect to the identification and implementation of security protection on each specific communication link. In return, the AESO expects that each applicable Responsible Entity will provide a document outlining their responsibilities in implementing security protection on each specific communication link. The AESO expects to include in its plan the responsibilities outlined by each applicable Responsibility in the AESO's document.

9 Development of Plans (section 3 (R1) of CIP-012-AB-1)

The AESO provides the following guidance in developing plans required for Requirement R1 of CIP-012-AB-1. However, each Responsible Entity has the discretion to follow a different plan.

1. Assess and document applicable control centres – perform an assessment to determine the control centres that have a communication link with another control centre, regardless of ownership of the control centres
    a. Assess, identify, and document any control centre that meet the exemption criteria
2. Assess and document applicable communication links between control centres – perform an assessment to determine each communication link between the applicable control centres
3. Assess and document the data being exchanged between the control centres – perform an assessment to determine the data that is being transmitted and received between control centres via each applicable communication link.
4. Assess and document the security protection scope for applicable communication links – using the assessments performed in Items 1 to 3 above, determine if the data being exchanged is in-scope for security protection as per Requirement R1.1 of CIP-012-AB-1.
    a. If the data being exchanged is in-scope, then each communication link used for the data exchange will be in-scope of CIP-012-AB-1.
    b. If the communication link is in-scope, then each control centre at either end of the communication link will be in-scope of CIP-012-AB-1.
5. Assess, identify, and document the security protection used – perform an assessment to determine the best feasible security protection for each of the applicable communication links
    a. If an in-scope communication link is between control centres owned by 2 different Responsible Entities, work with each other in identifying the best feasible security protection for the specific communication link
    b. Identify which applicable communication links will have physical security protection applied. Refer to guidance provided in the NERC documents and this information document.
    c. Identify which applicable communication links will have logical security protection applied. Refer to one or more of the following in determining the best feasible logical security protection: internal IT/OT security standards, practices, or policies; IT/OT cyber security standards, practices, or policies; and IT/OT network encryption standards, practices, or policies. Entities may also refer to industry best practices for identifying the best feasible logical security protection
6. Assess, identify, and document where the chosen security protection will be applied by performing an

assessment to determine the best feasible location for applying the chosen security protection for each of the applicable communications links

   a. For communication links that will have physical security protection applied, identify and document where the physical security protection will be applied. Identify and document the physical location in the entity's control centre floor plans and network diagrams

   b. For communication links that will have logical security protection applied, identify and document where the logical security protection will be applied. Identify and document the devices in the network diagrams where the logical security protection will be applied

7. Identify and document the responsibilities of each entity with respect to applying security protection for one or more applicable communication link

   a. For the communication links between your entity control centre and another Responsible Entity control centre, document your responsibility and the other entity's responsibility with respect to applying security protection for this specific communication link

   b. For the communication links between your entity control centres (between primary and backup control centres), document your responsibility with respect to applying security protection for this specific communication link

8. Include supporting documentation such as network diagrams, control centre floor plans and letters from responsible entities identifying their responsibilities for applying security protection.

9. Include a periodic review of the plan

10. Include business process to identify security protection implementation requirements for new connections with existing or new entities, to ensure the security protection is implemented at time of installation of new connections

Revision History

Posting Date	Description of Changes
13-09-2022	Initial Version