Technical Working Group on CIP-012-AB-1 Implementation

September 21, 2022

Notice

In accordance with its mandate to operate in the public interest, the AESO will be audio recording this session and making a discussion summary of the meeting available to the general public at www.aeso.ca. The accessibility of these discussions is important to ensure the openness and transparency of this AESO process, and to facilitate the participation of stakeholders. Participation in this session is completely voluntary and subject to the terms of this notice.

The collection of personal information by the AESO for this session will be used for the purpose of capturing stakeholder input for the Technical Working Group stakeholder sessions. This information is collected in accordance with Section 33(c) of the Freedom of Information and Protection of Privacy Act. If you have any questions or concerns regarding how your information will be handled, please contact the Director, Information and Governance Services at 2500, 330 – 5th Avenue S.W., Calgary, Alberta, T2P 0L4, by telephone at 403-539-2528, or by email at privacy@aeso.ca.

Asking questions in a virtual session

- Please introduce yourself including your organization
- If you are accessing the session via your computer or smartphone

  1. Click the “Raise Hand” icon and the host will be notified that you have a question
     - *When it is your turn to ask a question, the host will unmute your microphone, you in turn will need to unmute your microphone before you can ask your question. Your name will appear on the screen, but your camera will remain turned off*
  2. You can also ask questions by clicking on the “Q&A” icon and typing them in. Please include your organization when typing your question into the Q&A

- If you are accessing session via conference call
  - If you would like to ask a question press *5 on your phone’s dial pad and the host will see that you have raised your hand
  - When it is your turn to ask a question, the host will unmute your microphone, you in turn will need to unmute your microphone by hitting *6 on your phone’s dial pad before you can speak. Your number will appear on the screen

Welcome and introductions

- Daniela Cismaru, Director External Compliance Monitoring
- Haithem Al-Salam, Manager IT Audit Compliance and Controls
- Kathryn Kuber, Reliability Standards Technical Specialist
- Visu Viswanathan, Manager Operations Systems Data Management

Agenda

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

Session purpose and objectives

- Purpose
  - Engage stakeholders in discussions about the recently approved reliability standard CIP-012-AB-1, *Cyber Security - Communications between Control Centres* (“CIP-012-AB-1”)
- Session objectives
  - 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

Registrants (as of September 14, 2022)

- AltaLink Management Ltd.
- Ampere Industrial Security
- ATCO Electric Ltd.
- BluEarth Renewables
- Capital Power
- City of Lethbridge
- City of Medicine Hat
- ENMAX Energy Corp.
- ENMAX Power Corp.
- EPCOR Distribution & Transmission Inc.
- Lionstooth Energy Inc.
- Market Surveillance Administrator
- Neoen
- Suncor Energy Inc.
- TransAlta Corporation
- WSP

AESO Stakeholder Engagement Framework

OUR ENGAGEMENT PRINCIPLES

Inclusive and Accessible

Strategic and Coordinated

Transparent and Timely

Customized and Meaningful

Stakeholder participation

- The participation of everyone here is critical to the engagement process. To ensure everyone has the opportunity to participate, we ask you to:
  - Listen to understand others’ perspectives
  - Disagree respectfully
  - Balance airtime fairly
  - Keep an open mind

Reliability Standard CIP-012-AB-1, *Cyber Security – Communications between Control Centres* (“CIP-012-AB-1”)

CIP-012-AB-1 Purpose and Applicability

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.

Applicability

- This **reliability standard** applies to the following entities, referred to as "Responsible Entities":
- the **operator** of a **generating unit**;
- the **legal owner** of a **generating u**nit;
- the **operator** of an **aggregated generating facility**;
- the **legal owne**r of an **aggregated generating facility**;
- the **operator** of a **transmission facility**;
- the **legal owner** of a **transmission facility**; and
- 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**.

https://www.aeso.ca/rules-standards-and-tariff/alberta-reliability-standards/cip-012-cyber-security-communications-between-control-centres/download/CIP-012-AB-1.pdf

CIP-012-AB-1 Requirement R1

- **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

https://www.aeso.ca/rules-standards-and-tariff/alberta-reliability-standards/cip-012-cyber-security-communications-between-control-centres/download/CIP-012-AB-1.pdf

AESO Information Document 2021-007, *Cyber Security – Communications between Control Centres (ID #2021-007)*

Purpose

- 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 in implementing CIP-012-AB-1
- NERC Guidance Documents for CIP-012-1
  - *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")

Real-time assessment meaning

- An evaluation of system conditions using real-time data to assess pre-**contingency** and potential post-**contingency** operating conditions
- The assessment must 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

Real-time assessment data examples

- 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

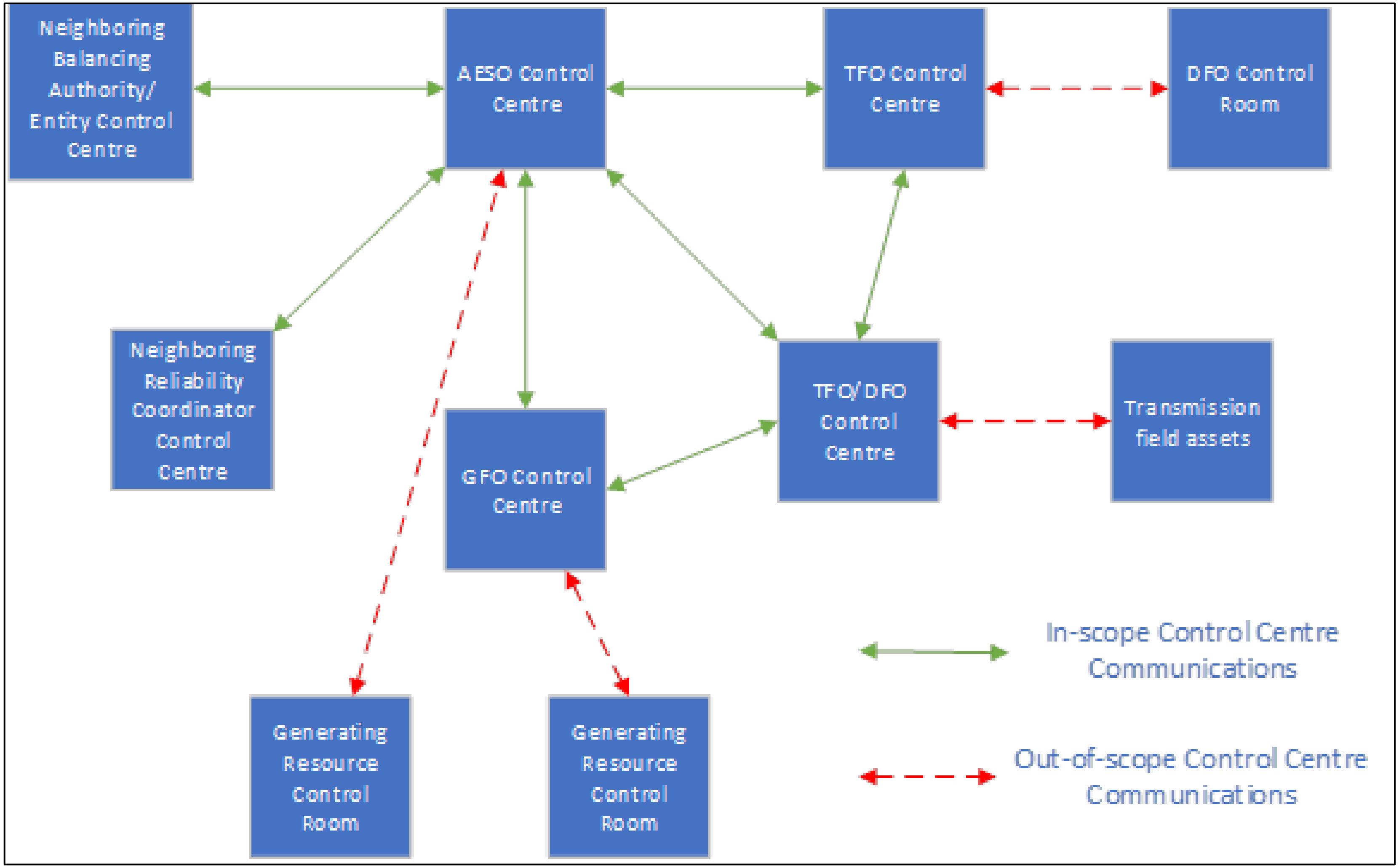
Real-time monitoring meaning

- Not defined by NERC
- 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

Real-time monitoring examples

- 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.

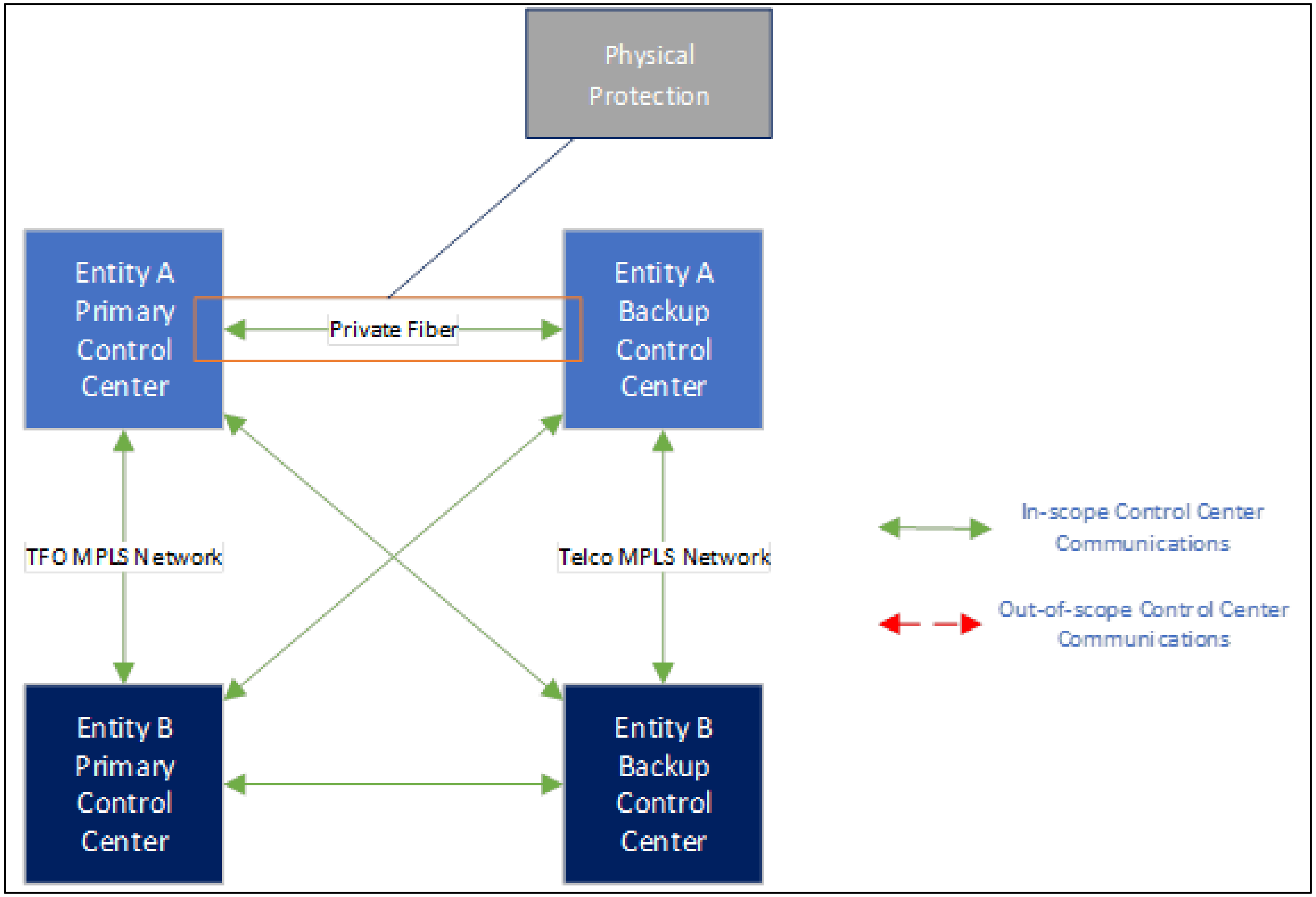
Applicable communication links reference model


Neighboring Balancing Authority/ Entity Control Centre
AESO Control Centre
TFO Control Centre
DFO Control Room
Neighboring Reliability Coordinator Control Centre
GFO Control Centre
TFO/DFO Control Centre
Transmission field assets
In-scope Control Centre Communications
Out-of-scope Control Centre Communications
Generating Resource Control Room
Generating Resource Control Room

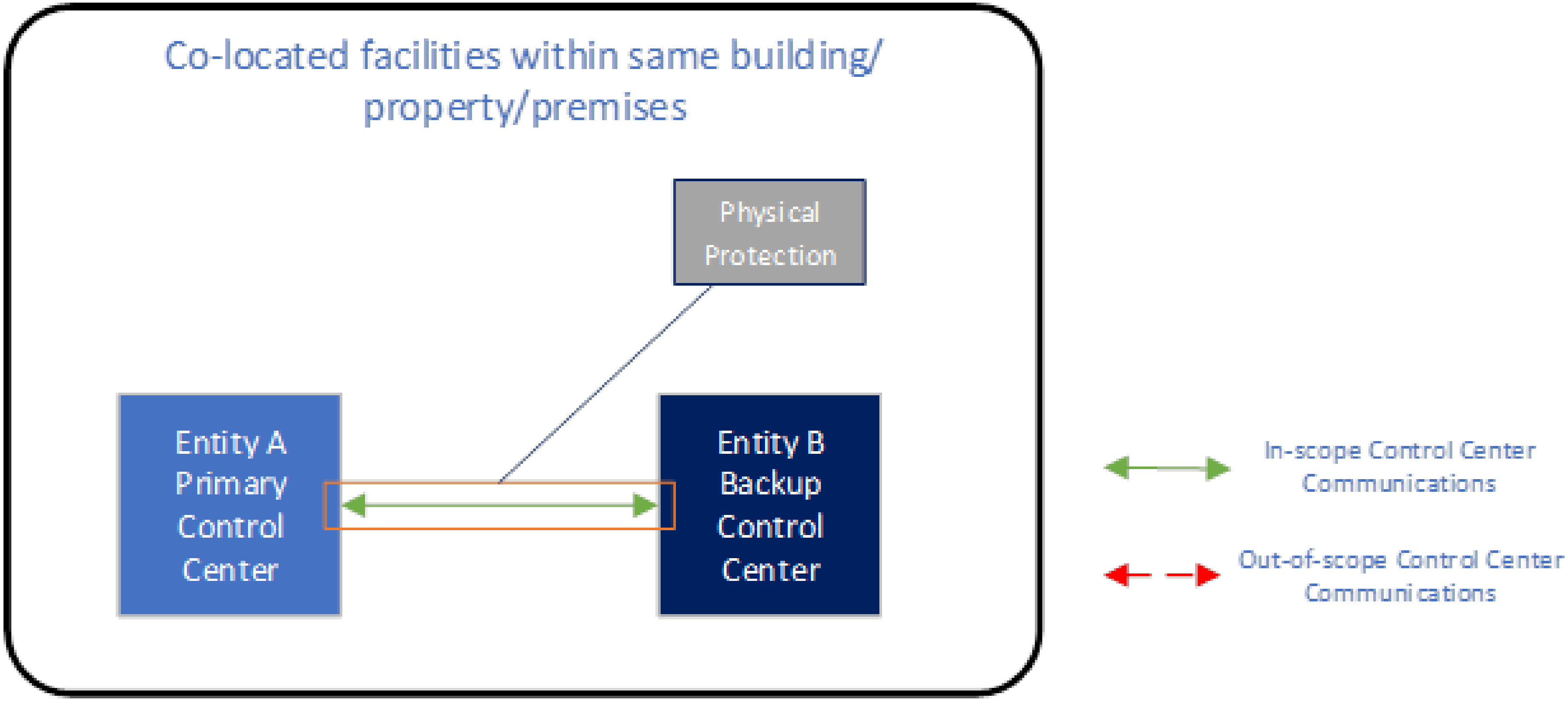
Identification of security protection

- Physical Protection
  - Access controlled, physical cable tamper protection
- Logical Protection
  - Encryption
- Combination of Physical and Logical
- Other
  - Application based protection

Scenarios where physical protection is appropriate

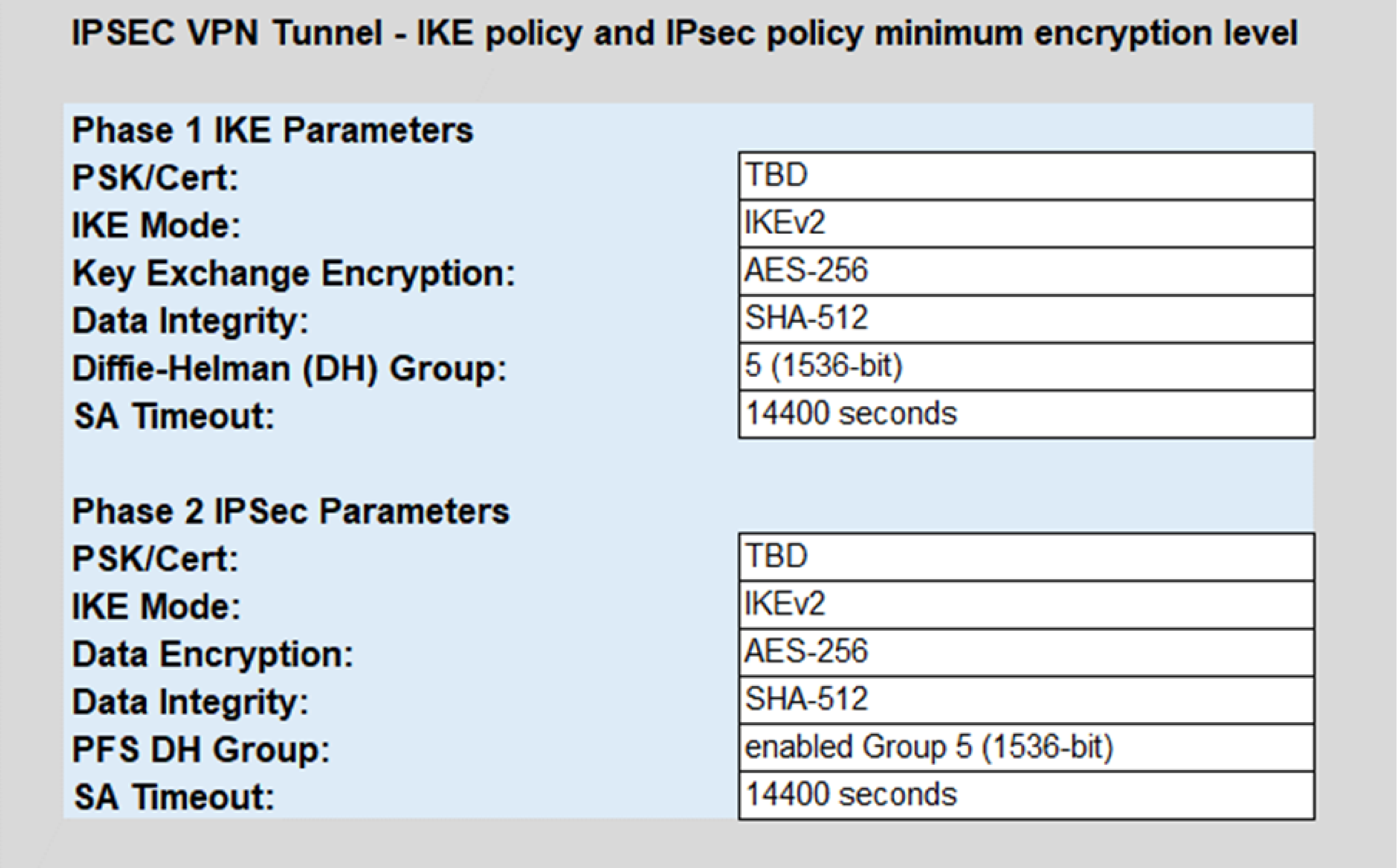

Physical Protection
Entity A Primary Control Center
Private Fiber
Entity A Backup Control Center
TFO MPLS Network
Telco MPLS Network
Entity B Primary Control Center
Entity B Backup Control Center
In-scope Control Center Communications
Out-of-scope Control Center Communications

Scenarios where physical protection is appropriate


Co-located facilities within same building/ property/premises
Physical Protection
Entity A Primary Control Center
Entity B Backup Control Center
In-scope Control Center Communications
Out-of-scope Control Center Communications

AESO's security protection for applicable links

- For applicable communication links between AESO and other Responsible Entity’s control centre

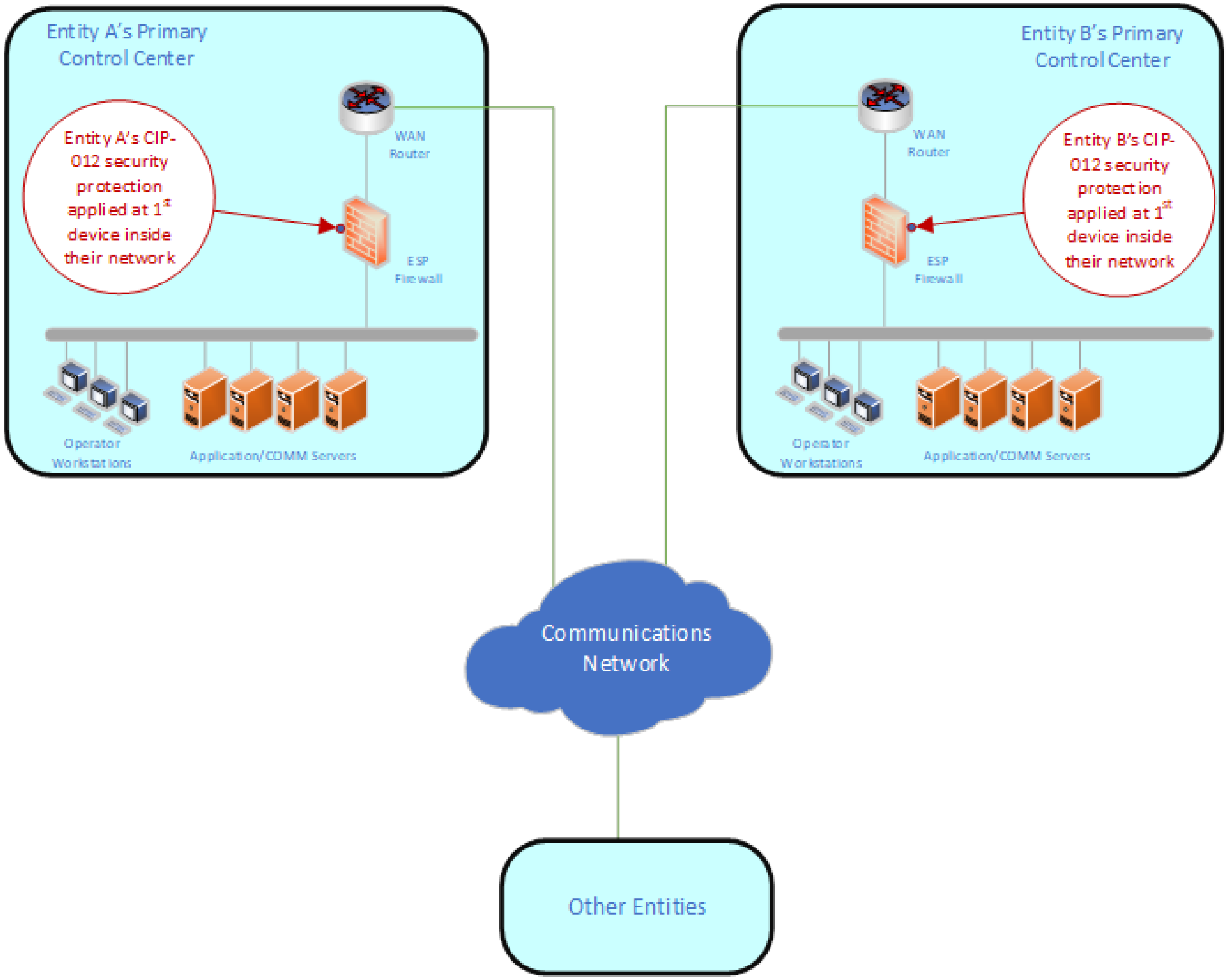


IPSEC VPN Tunnel - IKE policy and IPsec policy minimum encryption level

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

Identification of security protection location

- For logical protection


Entity A's Primary Control Center
Entity A's CIP-012 security protection applied at 1st device inside their network
WAN Router
ESP Firewall
Operator Workstations
Application/COMM Servers
Entity B's Primary Control Center
Entity B's CIP-012 security protection applied at 1st device inside their network
WAN Router
ESP Firewall
Operator Workstations
Application/COMM Servers
Communications Network
Other Entities

Identifying each other's responsibilities

- When control centres are owned or operated by different entities
- Exchange documents indicating responsible entity's ownership or responsibilities for a specific communication link
- Example:
  - Entity A acknowledges for the telecommunication link between Entity A and Entity B that is applicable to CIP-012-AB-1, Entity A has identified [type of security protection] to be implemented at [location of security protection implementation]
- Include other entity’s documents/confirmation of responsibilities in the plan

Guidance on developing the plan

- Identify applicable control centres
- Identify applicable communication links between control centres
- Identify the data being exchanged between the control centres
- Identify the security protection scope for applicable communication links
- Identify the security protection to be used
- Identify where the chosen security protection will be applied
- Identify the responsibilities of each entity

Guidance on developing the plan (cont.)

- Include supporting documentation such as network diagrams, control centre floor plans
- Include a periodic review of the plan
- 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

Questions?

AESO’s Key Learnings on Its CIP-012-AB-1 Implementation

AESO implementation lessons learned

- **Lesson #1: Network Configuration Responsibilities**
  - Responsibilities for network configuration may be distributed across multiple teams, including an external service provider
  - Document the process and responsibilities, do not assume it is clear for all parties

AESO implementation lessons learned (cont.)

- **Lesson #2: Start early, implementation may take longer than expected**
  - Alignment between a diverse group of entities with varying capabilities
  - Documentation and evidence collection
  - Assessment of risks and internal controls for ongoing compliance

AESO implementation lessons learned (cont.)

- **Lesson #3: What works for one communication link may not work for another**
  - Perform assessments of each link early and identify capabilities and restrictions for each link
  - Hardware configuration capabilities may be limited

AESO implementation lessons learned (cont.)

- **Lesson #4: encryption is not always be the most effective/feasible**
  - CIP-012-AB-1 does not require a specific type of protection
  - If encryption is not feasible today, implement physical protection or other protection while working towards encryption protection for future

Questions?

CIP-012-AB-1 Reliability Standards Audit Worksheet

Questions?

Next Steps and Session Close-Out

Next steps

- September 2022 | Initiate one-on-one detailed technical discussions between the AESO and applicable entities
- October 14, 2022 | Stakeholder feedback due
- October 21, 2022 | Post Stakeholder feedback received
- November 2022 | Post CIP-012 TWG discussion summary
- November 2022 | Stakeholder feedback gathered will be reviewed and considered for updates to the AESO ID #2021-007 and RSAW
- December 2022 | Post any updates to AESO ID #2021-007 and RSAW

Request for feedback

- We invite all interested stakeholders to provide their detailed input on this session via the questions set out in the **Stakeholder Comment Matrix TWG CIP-012 September 2022 on or before October 14, 2022.** The comment matrix is available on our website at www.aeso.ca
  - Path: Rules, Standards and Tariff > Alberta Reliability Standards > TWG CIP-012-AB-1 Implementation

Session close-out

- We want to thank you for attending the TWG on CIP-012-AB-1 Implementation and we would appreciate your feedback on the session
- Launch poll
  - The purpose of the session was clear
  - The information was presented in a clear manner
  - The presentation content was clear and informative
  - I found this session valuable

Questions?

Contact the AESO

- ***Twitter:*** *@theAESO*
- ***Email:*** *info@aeso.ca*
- ***Website:*** *www.aeso.ca*
- Subscribe to our stakeholder newsletter

Thank you

Appendix - Acronyms

Acronyms

- AUC = Alberta Utilities Commission
- DFO = Legal Owner of an Electric Distribution System
- GFO = Legal Owner of a Generating Unit or Aggregated Generating Facility
- IPsec = Internet Protocol Security
- MPLS = Multiprotocol Label Switching
- NERC Implementation Document = *Cyber Security – Communications Between Control Centers Implementation Guidance for CIP-012-1,* March 2020 version
- NERC Rationale Document = *Cyber Security – Communications between Control Centers Technical Rationale and Justification for Reliability Standard CIP-012-1,* August 2018 version
- TFO = Legal Owner of a Transmission Facility
- VPN = Virtual Private Network
- WAN = Wide-area Network