December 9, 2022

To: Market Participants and Other Interested Parties

Re: Consultation Letter on the following:

1) **Proposed new CIP-013-AB-2, *Cyber Security – Supply Chain Risk Management* ("CIP-013-AB-2")**
2) **Proposed new CIP-003-AB-8, *Cyber Security – Security Management Controls* ("CIP-003-AB-8")**
3) **Proposed new CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7")**
4) **Proposed new CIP-010-AB-4, *Cyber Security – Configuration Change Management and Vulnerability Assessments* ("CIP-010-AB-4")**
5) **Proposed retirement of existing CIP-003-AB-5, *Cyber Security – Security Management Controls* ("CIP-003-AB-5")**
6) **Proposed retirement of existing CIP-005-AB-5, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-5")**
7) **Proposed retirement of existing CIP-010-AB-1, *Cyber Security – Configuration Change Management and Vulnerability Assessments* ("CIP-010-AB-1")**

[items 1) through 4) are collectively referred to as the "CIP-013 and Supporting Standards"]

Section 19 of the *Transmission Regulation* requires the Alberta Electric System Operator ("AESO") to: (i) consult with stakeholders likely to be directly affected by the AESO's adoption or making of reliability standards ("Stakeholders"); and (ii) forward the proposed reliability standards to the Alberta Utilities Commission ("Commission") for review along with the AESO's recommendation that the Commission approve or reject them.[1]

Accordingly, the AESO is initiating Stakeholder engagement and seeking an initial round of comments from Stakeholders on the CIP-013 and Supporting Standards.

Background

Prioritization of CIP Standards

The AESO and Stakeholders have agreed that aligning the Critical Infrastructure Protection ("CIP") standards to the latest NERC versions is a top priority for industry. Increasing and evolving cyber threats are a high risk to the Alberta interconnected electric system ("AIES"), requiring the AESO and market participants to keep pace with security baselines and the latest technologies integrated in the updated CIP standards.

[1] Further information on the framework for reliability standards generally in Alberta can be found at https://www.aeso.ca/rules-standards-and-tariff/alberta-reliability-standards/.

Alberta Electric System Operator

www.aeso.ca

Calgary Place, 2500, 330-5th Avenue SW Calgary, AB T2P 0L4

Phone: 403-539-2450 | Fax: 403-539-2949

THE FUTURE OF ELECTRICITY

Through the ARS Program Enhancement Initiative, the AESO is currently undertaking significant enhancements to the ARS Program Lifecycle. To bridge the gap between current state and future state, the AESO is using the CIP standards to pilot aspects of the proposed risk-based approach and proposed enhancements to the ARS Program Lifecycle. The intent is to identify the methods that streamline the development and implementation of reliability standards through a "test and learn" approach and seek continuous feedback from Stakeholders as the consultation evolves.

At its November 21, 2022 Stakeholder session, the AESO shared its three-phase approach to new and upgraded CIP standard development:

- Phase 1: CIP-013 pilot incorporating dependent standards (CIP-003, CIP-005, CIP-010).
- Phase 2: CIP-004 and CIP-011;
- Phase 3: Align remaining CIP standards with latest NERC versions.

CIP-013-AB-2 and the Supporting Standards

The CIP-013 and Supporting Standards are focused on addressing new cyber security challenges facing the AIES:

- CIP-013-AB-2 introduces supply chain security. This reliability standard will mitigate cyber security risks to the reliable operation of the bulk electric system ("BES") by implementing security controls for supply chain risk management of BES Cyber Systems.
- CIP-003-AB-8, CIP-005-AB-7, and CIP-010-AB-4 each have associated changes that support supply chain security:
    - CIP-003-AB-8 changes specify consistent and sustainable security management controls that establish responsibility and accountability for the protection of BES Cyber Systems;
    - CIP-005-AB-7 changes manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems; and
    - CIP-010-AB-4 changes seek to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems.

Together, these four reliability standards will require all Responsible Entities with high-, medium-, and low-impact BES cyber systems to implement supply chain security.

Applicability

The CIP-013 and Supporting Standards apply to the following entities, referred to as "Responsible Entities":

- the legal owner of an electric distribution system that owns one or more of the following facilities, systems and equipment:
    - Certain underfrequency and under voltage load shed systems;
    - Certain remedial action schemes;
    - Certain protection systems;
- the operator of a generating unit that is part of the bulk electric system ("BES");

- the operator of an aggregated generating facility that is part of the BES;
- the operator of a transmission facility;
- the legal owner of a transmission facility; and
- the ISO.

Stakeholders are encouraged to refer to the CIP-013 and Supporting Standards for further detail on the applicability of each reliability standard.

Summary of Proposed Changes

The AESO is proposing to adopt the NERC versions of the CIP-013 and Supporting Standards with only the necessary revisions to align with Alberta-specific defined terms. The AESO is also proposing to adopt the NERC definitions of:

- Transient cyber asset; and
- Removable media.

However, the AESO is specifically interested in Stakeholder views on further revisions to the content of the reliability standards that may be necessary to effectively implement the CIP-013 and Supporting Standards in Alberta.

As identified in the *ARS Program Interim Work Plan*,[2] the AESO is targeting a Q4 2024 implementation timeline to address evolving risks to the security and reliability of the AIES. However, the AESO understands that market participants need to be able to plan and budget resources effectively to implement new and updated CIP standards and has requested specific comments on whether this is a reasonable timeline from the point of view of Stakeholders.

Stakeholder Engagement Schedule

Below is the proposed schedule for Stakeholder engagement:

Target Date	Consultation Step
February 1, 2023	Initial Stakeholder written comments on CIP-013 and Supporting Standards due
Mid-March 2023	First Stakeholder Reliability Standards Workshop focused on addressing initial Stakeholder written comments
April 2023	Second Stakeholder Reliability Standards Workshop (if necessary)
May 2023	Final Stakeholder written comments on CIP-013 and Supporting Standards (if necessary)
End of Q2 2023	AESO posts replies to stakeholders (if necessary) CIP-013 and Supporting Standards forwarded to the Commission.

The AESO is seeking an initial round of written comments from Stakeholders on the drafts of the CIP-013 and Supporting Standards to understand the key questions and concerns relating to reliability standard content, implementation, or compliance. The AESO's intent is to tailor consultation to effectively focus on these key areas and specifically use the Reliability Standards Workshops to discuss and collaborate with Stakeholders. However, the AESO is committed to maintaining a flexible approach and may alter the consultation steps if there is a more effective and efficient way to manage priorities and achieve objectives.

[2] https://www.aeso.ca/assets/Uploads/ars/RSDG/20OCT2022-ARS-Program-Interim-Work-Plan.pdf

Request for Comment

The AESO is providing a comment matrix to organize feedback on the CIP-013-AB-2 and Supporting Standards in the form of the attached *Stakeholder Comment Matrix*.

The CIP-013 and Supporting Standards Reference Material is a consolidated table with links to industry guidance material that Stakeholders may find useful in their review. While the reference materials currently contain NERC Reliability Standard Audit Worksheets ("RSAW"), the AESO will provide Stakeholders with Alberta-specific draft RSAWs in advance of the first Reliability Standards Workshop.

The deadline for Stakeholders to provide comments to ars_comments@aeso.ca, as noted above, is February 1, 2023. When submitting comments to the AESO, Stakeholders should ensure that comments provided represent all interests within their organization. The AESO will publish all Stakeholder comments received by the deadline.

Related Materials

The following documents are posted on the stakeholder engagement page:

1. Concordance Document;
2. *Stakeholder Comment Matrix* for CIP-013-AB-2 and Supporting Standards;
3. Blackline and clean copies of CIP-003-AB-8;
4. Blackline and clean copies of CIP-005-AB-7;
5. Blackline and clean copies of CIP-010-AB-4;
6. Blackline and clean copies of CIP-013-AB-2; and
7. CIP-013 and Supporting Standards Reference Material.

Sincerely,

Murray Mueller

Murray Mueller
Director, Operations Systems
Email: ars_comments@aeso.ca