

Information Document

Reasons for Access Rules and Ports Opening

ID #2019-053



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(s)¹ in effect, the Authoritative Document(s) governs.

1 Purpose

This Information Document relates to the following Alberta reliability standards:

- CIP-005-AB-5, *Electronic Security Perimeter(s)* (“CIP-005-AB-5”); and
- CIP-007-AB-5, *Cyber Security – System Security Management* (“CIP-007-AB-5”).

The purpose of this Information Document is to provide clarity to market participants with respect to the AESO’s interpretation of the reasons for access rules and ports opening, and the documented processes as it relates to the noted Critical Infrastructure Protection (“CIP”) standards.

2 Clarification of documented processes

The reference made to documented processes in R1 of CIP-005-AB-5 and Requirement R1 of CIP-007-AB-5 includes how to determine the reason or need. Determination may be made using: documented criteria; consultation with subject matter experts or vendors; vendor documentation or any other appropriate means. The determined reason or need is expected to be documented clearly in relation to the business function.

3 Clarification of reasons for granting access for CIP-005-AB-5 R1.3

For clarity, the reference made to “inbound and outbound access permissions” on an electronic access point in Requirement R1.3 of CIP-005-AB-5, should collectively consider:

- (i) the source device and/or service IP address, name or application;
- (ii) the destination device and/or service IP address, name or application; and
- (iii) the reason for granting access in relation to the business function.

4 Clarification of reasons for ports opening for CIP-007-AB-5 R1.1

For clarity, the reference made to “logical network accessible ports” in Requirement R1.1 of CIP-007-AB-5, should collectively consider:

- (i) the impacted device name or application;
- (ii) the protocol (e.g. TCP, UDP);
- (iii) the port or port range (e.g. 80, 1024-1029);
- (iv) the service name(s) (e.g. SSH); and
- (v) the justification of need in relation to the business function.

¹ “Authoritative Documents” 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. AESO Authoritative Documents include: the ISO rules, the Alberta reliability standards, and the ISO tariff.

Where vendor documentation specifies that a port or port range is used but does not provide its justification of need, and the vendor will not provide its justification of need, it is reasonable to justify the port or port range usage as required by the application. The vendor documentation or a vendor attestation is sufficient to support this documented need.

Revision History

Posting Date	Description of Changes
2019-12-03	Initial release of new ID