Information Document
CIP-004 Clarification
ID #2017-003RS

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 Authoritative Document:

- Alberta reliability standard CIP-004-AB-5.1, *Cyber Security – Personnel & Training* ("CIP-004").

The purpose of this Information Document is to provide clarification:

- regarding the use of the defined term "electronic access control and monitoring systems;
- on the use of "Responsible Entity's personnel" as it applies to requirement R1 Part 1.1; and
- on the use of "authorize based on need" as it applies to requirement R4 Part 4.1.

2 Electronic access control and monitoring systems

Where the defined terms "electronic access control and monitoring systems" are used, refer to the definition of "electronic access control or monitoring systems" [emphasis added to both].

The AESO will update all references to be "electronic access control and monitoring systems" in CIP-004 in due course.

3 Responsible Entity's personnel

For the purposes of requirement R1 Part 1.1 of CIP-004, the AESO considers the Responsible Entity's personnel, to include any person, regardless of their relationship to the Responsible Entity, who has authorized electronic or authorized unescorted physical access to the Responsible Entity's BES cyber systems.

4 Authorize based on need

As described in Section 2 of the Information Document, *Guidance Information for CIP Standards* ID #2015-003RS, the AESO may use the North American Electric Reliability Corporation ("NERC") CIP Guidance Information as reference material in assessing compliance with the CIP Standards. For the purposes of requirement R4 Part 4.1 of CIP-004, the AESO applies the guidance provided by NERC in its Guidelines and Technical Basis as follows:[2]

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

The AESO recommends that evidence to support the minimum necessary access privileges for performing assigned work functions be provided. Examples of evidence may include criteria for assessing need, role based provisioning, or demonstration of consistent provisioning performed by the same person.

[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 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.

[2] NERC CIP-004-5.1 – Cyber Security – Personnel & Training, Guidelines and Technical Basis, Section 4 – Scope of Applicability of the CIP Cyber Security Standards, page 43.
https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-5_1.pdf

Revision History

Posting Date	Description of Changes
2017-04-26	Initial release
2019-01-09	Updated to rename the Information Document, to remove the reference to the “Critical Infrastructure Protection terms and definitions”; and to add section 3 in relation to clarification on the use of Responsible Entity’s personnel.
2019-08-28	Updated to add section 4 in relation to clarification on the use of “authorize based on need”.