Information Document
Identifying, Protecting and Securely Handling BES Cyber System Information
ID #2020-017

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:

- Alberta Reliability Standard *CIP-011-AB-1, Cyber Security – Information Protection* ("CIP-011").

The purpose of this information document is to provide clarification:

- on the methods to identify information that meets the definition of BES cyber system information as it applies to requirement R1 Part 1.1; and
- on the procedures for protecting and securely handling BES cyber system information, including storage, transit, and use as it applies to requirement R1 Part 1.2.

2 Identify BES Cyber System Information

Responsible entities have flexibility in implementing requirement R1 Part 1.1. However, the AESO expects a responsible entity to explain the method(s) used for identifying information that meets the BES cyber system information definition. The AESO expects a responsible entity to provide sufficient guidance on how the responsible entity and its personnel identify BES cyber system information. This guidance may include using a process, classification, or criteria.

3 Procedures for Protecting and Securely Handling BES Cyber System Information

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 (the "NERC") CIP Guidance Information as reference material in assessing compliance with the CIP reliability standards. For the purposes of requirement R1 Part 1.2 of CIP-011, the AESO applies the guidance provided by the NERC in its Guidelines and Technical Basis within the NERC's *CIP-011-02, Cyber Security – Information Protection*. Please refer to the NERC's *CIP-011-02, Cyber Security – Information Protection* for more information.

The procedures for protecting and securely handling BES cyber system information, including storage, transit, and use, are expected to cover common use cases for protecting both physical and electronic information while it is being stored (e.g., physical storage), transmitted (e.g., across an unsecured network), or used (e.g., secure printing).

Revision History

Posting Date	Description of Changes
2020-08-14	Amended document title
2020-08-13	Initial release

[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 reliability standards, and the ISO tariff.