

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<sup>1</sup> in effect, the authoritative document governs.

### 1 Purpose

This information document relates to the following authoritative document:

- Alberta reliability standard CIP-009-AB-5 R1, *Cyber Security – Recovery Plans for BES Cyber Systems* (“CIP-009-AB-5”)

The purpose of this information document is to provide guidance to market participants with respect to the processes and data referenced in Part 1.5 of Table R1 – *Recovery Plan Specifications* (“Table R1”) in CIP-009-AB-5.

### 2 Processes to Preserve Data

Part 1.5 in Table R1 is primarily concerned with certain specific processes and data. Examples of material to be included in processes that would satisfy this requirement include:

- (a) reference to policies and programs that define the market participant’s data preservation strategy;
- (b) reference to other processes or procedures that provide further detail on how to execute on the data preservation strategy;
- (c) guidelines of the sequence and timing of critical activities required per cyber asset or capability; and
- (d) definition of the types of data required to determine the cause of a cyber security incident that triggers activation of any recovery plan.

Examples of data that may be preserved include the following:

- (e) security event logs;
- (f) locally hosted activity log files;
- (g) intrusion prevention and/or detection logs;
- (h) malicious code prevention logs;
- (i) network monitoring data; and
- (j) system health and state logs.

### Revision History

Posting Date	Description of Changes
2020-04-21	Initial release

<sup>1</sup> “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 reliability standards, and the ISO tariff.