Information Document
Guidance Information for CIP Standards
ID #2015-003RS

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 Documents:

- CIP-002-AB-5.1, *Cyber Security – BES Cyber System Categorization* ("CIP-002-AB-5.1");
- CIP-003-AB-8, *Cyber Security – Security Management Controls* ("CIP-003-AB-8");
- CIP-004-AB-5.1, *Cyber Security – Personnel & Training* ("CIP-004-AB-5.1");
- CIP-004-AB-7, *Cyber Security – Personnel & Training* ("CIP-004-AB-7");
- CIP-005-AB-5, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-5");
- CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7");
- CIP-006-AB-5, *Cyber Security – Physical Security of BES Cyber Systems* ("CIP-006-AB-5");
- CIP-007-AB-5, *Cyber Security – System Security Management* ("CIP-007-AB-5");
- CIP-008-AB-5, *Cyber Security – Incident Reporting and Response Planning* ("CIP-008-AB-5");
- CIP-009-AB-5, *Cyber Security – Recovery Plans for BES Cyber Systems* ("CIP-009-AB-5");
- CIP-010-AB-4, *Cyber Security – Configuration Change Management and Vulnerability Assessments* ("CIP-010-AB-4");
- CIP-011-AB-1, *Cyber Security – Information Protection* ("CIP-011-AB-1");
- CIP-011-AB-3, *Cyber Security – Information Protection* ("CIP-011-AB-3");
- CIP-013-AB-2, *Cyber Security – Supply Chain Risk Management* ("CIP-013-AB-2");
- CIP-014-AB-2, *Physical Security* ("CIP-014-AB-2"); and
- CIP-PLAN-AB-3, Cyber Security – *Implementation Plan for Version 5 CIP Security Standards* ("CIP-PLAN-AB-3").

(collectively, the "CIP Standards").

The purpose of this Information Document is to provide guidance on the CIP Standards. The main body of this Information Document contains information that is relevant to the CIP Standards listed above. Appendices 1 to 10 contain additional information that is relevant for specific CIP Standards.

This Information Document contains guidance on some future-effective standards, including CIP-003-

AB-8, CIP-004-AB-7, CIP-005-AB-7, CIP-010-AB-4, CIP-011-AB-3, and CIP-013-AB-2. Such guidance on future-effective standards will become applicable as of the effective date of the relevant standards.

[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 Use of NERC Guidance Material for the CIP Standards

Each Responsible Entity is responsible for determining for its facilities what actions are necessary to meet the requirements in the CIP Standards.

The AESO encourages each Responsible Entity to reference the NERC CIP guidance material as it implements the CIP Standards. In addition, the AESO plans to use the NERC CIP guidance material as reference material in assessing compliance with the CIP Standards where it determines that the NERC CIP guidance material is applicable. If the AESO determines that there are aspects of the NERC CIP guidance material that are not applicable in Alberta, then the AESO will list that information in this Information Document.

See Appendix 1 – *Additional CIP Guidance Material* for key document references.

Appendices

Appendix 1	*Additional CIP Guidance Material*
Appendix 2	*Clarification Related to Industrial Complexes*
Appendix 3	*Identify, Assess, and Correct*
Appendix 4	*Reasons for Access Rules and Ports Opening*
Appendix 5	*Clarification on CIP-005-AB-7 Terms*
Appendix 6	*Clarification on Supply Chain Security Risk Management Plans*
Appendix 7	*Clarification on Vendors*
Appendix 8	*Clarification on CIP-004-AB-7*
Appendix 9	*Clarification on Implementation Plan for CIP-003-AB-8*
Appen*dix 10*	*Early Compliance Option for CIP-004-AB-7 and CIP-011-AB-3*

Revision History

Posting Date	Description of Changes
2024-05-23	Updated the document with the latest version of CIP-004 and CIP-011 through out this ID. Added Appendix 10 to include Early Compliance Option for the latest version of CIP-004 and CIP-011. Updated Appendix 1 to add guidance material references for CIP-004-AB and CIP-011-AB, including NERC guidance material repeated in ID#2018-003RS, CIP-004 Clarification (“ID#2018-003RS”) and ID #2020-017, Identifying, Protecting and Securely Handling BES Cyber System Information (“ID#2020-017”). Retired ID#2020-017. Removed NERC content from ID#2018-003RS. Moved remaining content from ID#2018-003RS to Appendix 8. Updated Appendix 3, removed CIP-004-AB-7 and CIP-011-AB-3 from the applicability. Added Appendix 9 to provide clarification on implementation plan for CIP-003-AB-8.

2023-09-25	Addition of CIP-013-AB-2 to Section 1. Updated versions of CIP-003, CIP-005, CIP-010, and CIP-PLAN in Section 1. Modified document structure to have the main body contain information related to all applicable CIP Standards of the document and Appendices 1 to 7 contain additional information that is relevant for specific CIP Standards. The information found in these Appendices 1 to 7 is as follows: • Moved Section 3 *Clarification Regarding Industrial Complexes* of this ID#2015-003RS to Appendix 2. • Moved Section 5, *Identify, Assess, and Correct* of this ID#2015-003RS, to Appendix 3. • Moved all content from ID#2019-053, *Reasons for Access Rules and Ports Opening*, to Appendix 4. • Added Appendices 1, 5, 6, and 7 for specific information related to CIP-005-AB-7, CIP-010-AB-4, and CIP-013-AB-2. In addition, moved Section 4, *Clarification Regarding Applicability* of this Information Document, which provided clarification regarding the CIP Standards applicability statements 4.1.3 and 4.1.4, to general ARS Information Document, [ID# TBD]. Editorial updates made throughout the document to improve clarity.
2022-04-01	Addition of CIP-014-AB-2 to Section 1.
2019-12-03	Initial release of ID#2019-053, *Reasons for Access Rules and Ports Opening*.
2019-01-15	Deleted last sentence in Section 5 and amended additional sentence to minimize ambiguity.
2017-05-16	Addition of subsection 5.
2017-05-04	Addition of subsections 3 and 4.
2015-09-21	Initial publication of this ID (ID#2015-003RS, *Guidance Information for CIP Standards*).

Appendix 1

Additional CIP Guidance Material

This Appendix 1 includes specific information that provides information to Responsible Entities with respect to additional CIP guidance material.

NERC CIP guidance material can be found on the NERC website, and the NERC One-Stop Shop is a useful spreadsheet collating links to past and current versions of standards and some of their related documents. Table 1 provides a list of key CIP Standard guidance material.

Additional resources and guidance may be found from these sites:

- WECC / Program Areas / Compliance / US: WECC Compliance US (wecc.org)
- NATF / Industry-initiatives / supply-chain-industry-coordination: Supply Chain Industry Coordination (natf.net)
- NATF Documentation: Documents (natf.net)
- NERC Supply Chain Risk Mitigation Program (nerc.com)

Table 1: Key CIP Standard Guidance Material

Applicable Standard	Document Title	Source	Version/Date Published
CIP-004-5.1 CIP-004-7	Cyber Security — Personnel & Training Technical Rationale and Justification for Reliability Standard CIP-004-X	NERC	March 2021
CIP-004-7 CIP-011-3	CIP-004-7 R6 and CIP-011-3 R1 - Cloud Solutions for BCSI (RSTC)	NERC	June 21, 2023
CIP-004-7 CIP-011-3	Technical Reference Document - BCSI in the Cloud Tabletop Exercise	NERC	March 22,2023
CIP-004-7 CIP-011-3	Implementation Plan - Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011	NERC	June 2021
CIP-005-7	Cyber Security – Electronic Security Perimeter(s) Technical Rationale and Justification for Reliability Standard CIP-005-7, (”NERC CIP-005-7 Rationale Document”)	NERC	Oct 2020
CIP-010-4	Cyber Security — Configuration Change Management and Vulnerability Assessments Technical Rationale and Justification for Reliability Standard CIP-010-4	NERC	Oct 2020
CIP-010-3	NATF Software Integrity & Authenticity Implementation Guidance for CIP-010-3 R1 Requirement Part 1.6	NATF	Version 1.0 Approved Nov 6, 2017

CIP-011-1 CIP-011-3	Cyber Security – Information Protection Technical Rationale and Justification for Reliability Standard CIP-011-X	NERC	March 2021
CIP-011-3	Security Guideline: Primer for Cloud Solutions and Encrypting BCSI	NERC	10 June 2020
CIP-013-2	NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans	NERC	Version 1.1 Approved Oct 23, 2023
CIP-013-1	NATF CIP-013-1 Implementation Guidance	NERC	Version 2.0 Approved April 3, 2019
CIP-013-1	NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors	NERC	Version 3.1 Approved Oct 23, 2023
CIP-013-1	Cyber Security Supply Chain Risk Management Plans Implementation Guidance for CIP-013-1	NERC	Draft April 2017
CIP-005-6 CIP-010-3 CIP-013-1	Frequently Asked Questions Supply Chain – Small Group Advisory Sessions	NERC	May 05, 2021
CIP-013-1	CIP CMEP FAQs	NERC	-
CIP-013-2	Cyber Security – Supply Chain Risk Management Technical Rationale and Justification for Reliability Standard CIP-013-2, (”NERC CIP-013-2 Rationale Document”)	NERC	Oct 2020
CIP-013-2	Security Guideline: Cyber Security Risk Management Lifecycle	NERC	Dec 6, 2022
CIP-013-2	Security Guideline: Vendor Risk Management Lifecycle	NERC	March 22, 2023

Appendix 2

Clarification Related to Industrial Complexes

Appendix 2 provides specific information in relation to the following **reliability standards**[2]:

- CIP-002-AB-5.1, *Cyber Security – BES Cyber System Categorization* ("CIP-002-AB-5.1");
- CIP-004-AB-5.1, *Cyber Security – Personnel & Training* ("CIP-004-AB-5.1");
- CIP-004-AB-7, *Cyber Security – Personnel & Training* ("CIP-004-AB-7");
- CIP-006-AB-5, *Cyber Security – Physical Security of BES Cyber Systems* ("CIP-006-AB-5");
- CIP-007-AB-5, *Cyber Security – System Security Management* ("CIP-007-AB-5");
- CIP-008-AB-5, *Cyber Security – Incident Reporting and Response Planning* ("CIP-008-AB-5");
- CIP-009-AB-5, *Cyber Security – Recovery Plans for BES Cyber Systems* ("CIP-009-AB-5");
- CIP-011-AB-1, *Cyber Security – Information Protection* ("CIP-011-AB-1"); and
- CIP-011-AB-3, *Cyber Security – Information Protection* ("CIP-011-AB-3").

The purpose of this appendix is to provide specific information regarding facilities that are part of an industrial complex.

1 Generating Unit that is part of an Industrial Complex

Subsection 4.2.2.3.1. of the CIP Standards refers to a generating unit that is:

"directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 18 MW unless the **generating unit** is part of an industrial complex;"

For clarity, the wording "unless the **generating unit** is part of an industrial complex" is intended to indicate that, if the **generating unit** is part of an industrial complex, the only applicable subsection is 4.2.2.3.3. In other words, if the generating unit is part of an industrial complex, then the CIP Standards apply if the industrial complex has **supply transmission service** greater than 67.5 MW, unless the **generating unit** is a contracted **blackstart resource**, in which case subsection 4.2.2.3.4. is applicable to that **generating unit**.

2 Generating Unit that is within a Power Plant that is part of an Industrial Complex

Subsection 4.2.2.3.2.3. of the CIP Standards refers to a **generating unit** that:

"has a combined **maximum authorized real power** rating greater than 67.5 MW unless the power plant is part of an industrial complex;"

For clarity, the wording "unless the power plant is part of an industrial complex" is intended to indicate that, if the **generating unit** is within a power plant that is part of an industrial complex, the only applicable subsection is 4.2.2.3.3. In other words, if the **generating unit** is within a power plant that is part of an industrial complex, then the CIP Standards apply if the industrial complex has **supply transmission service greater** than 67.5 MW, unless the **generating unit** is a contracted **blackstart resource**, in which case subsection 4.2.2.3.4. is applicable to that **generating unit**.

3 Aggregated Generating Facility that is part of an Industrial Complex

Subsection 4.2.2.4.1. of the CIP Standards refers to an **aggregated generating facility** that is:

[2] Words and phrases in bold (excluding document titles) have the meanings given to them in the AESO's *Consolidated Authoritative Documents Glossary*, available at www.aeso.ca.

“directly connected to the **bulk electric system** and has a **maximum authorized real power** rating greater than 67.5 MW unless the **aggregated generating facility** is part of an industrial complex;”

For clarity, the wording “unless the **aggregated generating facility** is part of an industrial complex” is intended to indicate that, if the **aggregated generating facility** is part of an industrial complex, the only available subsection is 4.2.2.4.2. In other words, if the **aggregated generating facility** is part of an industrial complex, then the CIP Standards apply if the industrial complex has **supply transmission service** greater than 67.5 MW, unless the **aggregated generating facility** is a contracted **blackstart resource**, in which case subsection 4.2.2.4.3. is applicable to that **aggregated generating facility**.

Appendix 3

Identify, Assess, and Correct

Appendix 3 provides specific information to Responsible Entities with respect to "identify, assess and correct" language as it relates to the following **reliability standards**:

- CIP-004-AB-5.1, *Cyber Security – Personnel & Training* ("CIP-004-AB-5.1");
- CIP-006-AB-5, *Cyber Security – Physical Security of BES Cyber Systems* ("CIP-006-AB-5");
- CIP-007-AB-5, *Cyber Security – System Security Management* ("CIP-007-AB-5");
- CIP-009-AB-5, *Cyber Security – Recovery Plans for BES Cyber Systems* ("CIP-009-AB-5"); and
- CIP-011-AB-1, *Cyber Security – Information Protection* ("CIP-011-AB-1").

The requirement in a CIP Standard to "identify, assess and correct" is referred to as the "self-correcting" part of the requirement, and the underlying requirement is referred to as the "technical requirement".

The AESO recommends that Responsible Entities identify, assess and correct deficiencies in meeting the technical parts of these requirements as follows:

(a) identify deficiencies by self-reporting contraventions to the Market Surveillance Administrator ("MSA"); and

(b) assess and correct deficiencies that are the same as the first identified deficiency through a mitigation plan submitted to the MSA as described in the MSA Compliance Process.

The following evidence may be used to demonstrate that the self-correcting part of the requirement has been satisfied:

(i) evidence that the Responsible Entity is able to identify deficiencies in meeting the technical part of the requirement;

(ii) records of each identified deficiency in meeting the technical part of the requirement;

(iii) records of the result of an assessment made of each identified deficiency in meeting the technical part of the requirement;

(iv) records of the mitigating actions made to correct each identified deficiency in meeting the technical part of the requirements; and

(v) evidence that each identified deficiency in meeting the technical part of the requirement was corrected.

Appendix 4

Reasons for Access Rules and Ports Openings

Appendix 4 provides specific information to Responsible Entities 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 following **reliability standards**:

- CIP-003-AB-8, *Cyber Security – Security Management Controls* ("CIP-003-AB-8");
- CIP-005-AB-5; *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-5");
- CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7"); and
- CIP-007-AB-5, *Cyber Security – System Security Management* ("CIP-007-AB-5").

1 Clarification of documented processes

Requirement R1 of CIP-005-AB-7, Requirement R1 of CIP-007-AB-5, and Requirement R2 Attachment 1 Section 3 of CIP-003-AB-8 contain references made to documented processes that include 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.

2 Clarification of reasons for granting access for CIP-005-AB-7 R1.3 and CIP-003-AB-8 R2

For clarity, in Requirement R1.3 of CIP-005-AB-7, the reference made to "inbound and outbound access permissions" on an **electronic access point**, or Requirement R2 Attachment 1 Section 3 of CIP-003-AB-8 "inbound and outbound electronic access", 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.

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

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

(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.

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.

Appendix 5

Clarification on CIP-005-AB-7 Terms

Appendix 5 provides specific information to Responsible Entities with respect to terms used in the following **reliability standard**:

- CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7")

The AESO agrees with the *NERC CIP-005-7 Rationale Document*, including the interpretation of the terms "connection", "authenticate", and "control". The AESO's *Consolidated Authoritative Document Glossary* includes the defined term "interactive remote access".

In addition to the previous CIP-005-AB-5 Requirement R2 for **interactive remote access**, the new CIP-005-AB-7 "active vendor remote access (including **interactive remote access** and system-to-system remote access)" requires Responsible Entities to know about every vendor connection for the applicable systems (Requirement R2.4) and be able to disable those connections (Requirement R2.5). The applicable systems for Requirement R2.4 and Requirement R2.5 are High and Medium Impact **BES cyber systems** and their associated **protected cyber assets**. CIP-005-AB-7 Requirement R3 requires Responsible Entities to know about authenticated vendor initiated remote connections to **electronic access control or monitoring systems** and **physical access control systems** associated with High Impact **BES cyber systems** and Medium Impact **BES cyber systems** with **external routable connectivity** (Requirement 3.1) and be able to terminate those connections and control the vendors' ability to reconnect (Requirement 3.2).

Appendix 6

Clarification on Supply Chain Security Risk Management Plans

Appendix 6 provides specific information with respect to terms used in the following **reliability standards**:

- CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7");
- CIP-010-AB-4, *Cyber Security – Configuration Change Management and Vulnerability Assessments* ("CIP-010-AB-4"); and
- CIP-013-AB-2, *Cyber Security – Supply Chain Risk Management* ("CIP-013-AB-2").

In CIP-013-AB-2, the AESO expects that Responsible Entities will include the topics identified in Requirement R1.2.1 through R1.2.6 in their supply chain risk management plan(s) so that procurement and contract negotiation processes address the applicable risks. Responsible Entities may consider additional cyber security criteria in their supply chain risk management plan(s).

CIP-013-AB-2 Requirement R1 supply chain risk management plan(s) and Requirement R2 implementation would be applicable to all procurements of relevant products or services on or after the effective date of the standard. The AESO recommends that the risk assessment be performed on the vendor, product, and/or service as dictated by the Responsible Entity's supply chain risk management plan(s). The Responsible Entity's supply chain risk management plan(s) determine(s) where and how the risk assessment is performed.

For clarity, only procurements for applicable **BES cyber systems** that occur on or after the effective date of CIP-013-AB-2 are in scope for the CIP-013-AB-2 procurement planning processes. The requirements for CIP-005-AB-7 and CIP-010-AB-4 are still subject to their effective dates, including existing applicable **BES cyber systems**.

Appendix 7

Clarification on Vendors

Appendix 7 provides specific information with respect to the term "vendor" used in the following **reliability standards**:

- CIP-005-AB-7, *Cyber Security – Electronic Security Perimeter(s)* ("CIP-005-AB-7"); and
- CIP-013-AB-2, *Cyber Security – Supply Chain Risk Management* ("CIP-013-AB-2").

1 Clarification related to the term "vendor"

The AESO considers the term "vendor" to have the same meaning as described in both the NERC CIP-005-7 Rationale Document, Section *Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS*, and the NERC CIP-013-2 Rationale Document, Section *Rational for Requirement 1 and Requirement 2*:

> "The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

The AESO agrees with the NERC description that vendor includes all types of system integrators. By this description, an embedded contractor from a system integrator would not be considered part of the Responsible Entity.

2 Inclusion of Vendor in Supply Chain Risk Management Plan(s)

The AESO expects the Responsible Entity to document the scope of their use of the term "vendor", in their supply chain risk management plan(s) ensuring that it is broad enough to fulfill the intent of CIP-013-AB-2.

For Requirement R1 and Requirement R2 of CIP-013-AB-2 the AESO recommends that the Responsible Entity use its supply chain risk management plan(s) to identify and assess the risks associated for all procurements and installations of items such as third-party software or open-source software, where negotiated contracts with a vendor may not be possible. The results of this analysis would dictate what mitigations are appropriate to address the risks. Further, the Responsible Entity would be able to demonstrate that this due diligence was performed.

For Requirement R1 of CIP-013-AB-2, the AESO recommends that the Responsible Entity include in its supply chain risk management plan(s) the controls that will ensure awareness of possible vendor mergers, acquisitions, or transitions, as well as the steps they will take to identify, assess, and mitigate any risks of such situations. A "transition" refers to the transition of products or services from one vendor to another.

Appendix 8

CIP-004 Clarification

Appendix 8 provides specific information in relation to the following **reliability standard**:

- CIP-004-AB-5.1, *Cyber Security – Personnel & Training* ("CIP-004-AB-5.1"); and
- CIP-004-AB-7, *Cyber Security – Personnel & Training* ("CIP-004-AB-7").

The purpose of this appendix is to provide clarification: on the use of "Responsible Entity's personnel" as it applies to requirement R1 Part 1.1;

1 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**.

Appendix 9

Clarification on Implementation Plan for CIP-003-AB-8

Appendix 9 clarifies the method for calculating the percentage of applicable assets in the CIP-PLAN-AB-3 implementation plan, as it relates to the following **reliability standards**:

- CIP-002-AB-5.1, *Cyber Security – BES Cyber System Categorization* ("CIP-002-AB-5.1")
- CIP-003-AB-8, *Cyber Security – Security Management Controls* ("CIP-003-AB-8")
- CIP-PLAN-AB-3, *Cyber Security – Implementation Plan for CIP* ("CIP-PLAN-AB-3")

For the purposes of the CIP-PLAN-AB-3 implementation plan, Responsible Entities may calculate the percentage of assets compliant with Requirement R2 of CIP-003-AB-8 as follows:

$$Percent\ compliant = \frac{Applicable\ assets\ considered\ compliant\ and\ ready\ for\ audit}{Total\ applicable\ assets\ owned\ by\ Responsible\ Entity} \times 100$$

The AESO considers an applicable asset to be compliant with requirement R2 of CIP-003-AB-8 if all low impact BES cyber systems located at that applicable asset are compliant with requirement R2 of CIP-003-AB-8 R2.

1 Clarification related to the term "generating units"

For generating units and aggregated generating facilities, as set out in CIP-002-AB-5.1 requirement R1(iii), the AESO considers the whole generating resource to be one asset for the purposes of CIP-PLAN-AB-3. For example, a generating plant containing multiple generating units is considered to be one asset.

2 Clarification on the number of applicable assets

When calculating the number of compliant assets required to meet the timeline set out in CIP-PLAN-AB-3, Responsible Entities may round up to the nearest whole number.

For example: If a Responsible Entity has 9 total applicable assets as defined in Requirement R1 of CIP-002-AB-5.1, then the implementation timeline as required by CIP-PLAN-AB-3 is as follows:

- 15% of applicable assets by December 31, 2024 = 2 assets
- 30% of applicable assets by December 31, 2025 = 3 assets
- 60% of applicable assets by December 31, 2026 = 6 assets
- 100% of applicable assets on October 1, 2027 = 9 assets

Appendix 10

Early Compliance Option for CIP-004-AB-7 and CIP-011-AB-3

Appendix 10 provides specific information with respect to early compliance with the following **reliability standards**:

- CIP-004-AB-7, *Cyber Security – Personnel & Training* ("CIP-004-AB-7");
- CIP-011-AB-3, *Cyber Security – Information Protection* ("CIP-011-AB-3").

CIP-PLAN-AB-3 provides Responsible Entities with the option to comply early with CIP-004-AB-7 and CIP-011-AB-3, prior to the effective date of April 1, 2026. The Responsible Entity may only elect early compliance with both CIP-004-AB-7 and CIP-011-AB-3 together and not separately.

Responsible Entities who choose to elect the early compliance option will have to notify the AESO using the email address; rscompliance@aeso.ca. The Responsible Entity should provide the date it will be in compliance with CIP-004-AB-7 and CIP-011-AB-3 in the notification sent to the AESO. The AESO shall confirm receipt of notification to the Responsible Entity.

It is recommended that Responsible Entities provide the notification at least 7 **business days** prior to the date upon which the Responsible Entity wants to begin compliance with the new CIP-004-AB-7 and CIP-011-AB-3.

Responsible Entities that elect early compliance will be monitored for compliance with the new CIP-004-AB-7 and CIP-011-AB-3 beginning on the early compliance date provided to the AESO. The Responsible Entity is expected to continue compliance with the existing CIP-004-AB-5.1 and CIP-011-AB-1 until the date upon which the Responsible Entity wants to begin compliance with the new CIP-004-AB-7 and CIP-011-AB-3.