Alberta Reliability Standard
Cyber Security – Implementation Plan for CIP
CIP-PLAN-AB-3

1. Purpose

The purpose of this **reliability standard** is to set the effective dates for requirements of CIP Cyber Security **reliability standards** and describe compliance timelines for planned and unplanned changes that result in a higher categorization for a **BES cyber system**.

2. Applicable Reliability Standards

This **reliability standard** applies to the following CIP Cyber Security **reliability standards**:

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

(collectively referred to as "CIP Cyber Security **reliability standards**")

3. General Considerations

The intent of the *Initial Performance of Certain Periodic Requirements* section below is for each Responsible Entity, as defined in the applicable **reliability standard**, to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions.

The implementation of CIP-005-AB-7, CIP-010-AB-4, and CIP-013-AB-2 does not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers, or other entities executed as of the effective date of the **reliability standards**.

In implementing CIP-013-AB-2, Responsible Entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the Responsible Entity negotiates after the effective date, or direct procurements covered under the Responsible Entity's plan) that begin on or after the effective date of CIP-013-AB-2. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-AB-2.

4. Compliance with Reliability Standards

Once each new version of the CIP Cyber Security **reliability standards** becomes effective, in accordance with the *Effective Date* section below, the Responsible Entities identified in the applicability section of each version of the CIP Cyber Security **reliability standard** shall comply with the requirements of those **reliability standards**.

5. Effective Date

The CIP Cyber Security **reliability standards**, except for 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,became effective on October 1, 2017.

CIP-003-AB-8, with the exception of CIP-003-AB-8 requirement R2, CIP-005-AB-7, CIP-010-AB-4, and CIP-013-AB-2 become effective on October 1, 2024.CIP-003-AB-8, requirement R2 and CIP-004-AB-7 and CIP-011-AB-3 will become effective as set out in the implementation plans below.

Implementation plan for CIP-003-AB-8 R2

CIP-003-AB-8, requirement R2 shall be effective on the following timeline for all Responsible Entities:

- 15% of applicable assets by December 31, 2024;
- 30% of applicable assets by December 31, 2025;
- 60% of applicable assets by December 31, 2026; and
- 100% of applicable assets on October 1, 2027.

CIP-003-AB-5, requirement R2 shall remain effective throughout the phased implementation period of CIP-003-AB-8 R2. Each Responsible Entity must remain compliant with CIP-003-AB-5, requirement R2 until that entity meets the requirements of CIP-003-AB-8, requirement R2 in accordance with the Implementation Plan given above.

Early Implementation Plan for CIP-004-AB-7 and CIP-011-AB-3

CIP-004-AB-7 and CIP-011-AB-3 become effective on April 1, 2026. Each Responsible Entities, except for the **ISO,** may elect an earlier effective date following approval by the Alberta Utilities Commission and prior to April 1, 2026. Each Responsible Entities, except for the **ISO,** electing to comply with an earlier effective date shall notify the **ISO** of the date of compliance with the CIP-004-AB-7 and CIP-011-AB-3 **reliability standards** in writing.

The **ISO** may elect an earlier effective date following approval by the Alberta Utilities Commission and prior to April 1, 2026 by providing notice in writing to the Market Surveillance Administrator.

Each Responsible Entities shall comply with CIP-004-AB-5.1 and CIP-011-AB-1 until receipt of the notice confirming the elected earlier effective date..

6. Initial Performance of Certain Periodic Requirements

Specific CIP Cyber Security **reliability standards** have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to,

". . . at least once every 15 **months** . . .", and Responsible Entities shall initially comply with those periodic requirements as follows:

6.1. on or before the effective date of CIP Cyber Security **reliability standards** for the following requirements:

- CIP-002-AB-5.1, requirement R2;
- CIP-003-AB-8, requirement R1;
- CIP-004-AB-7, requirement R6, Part 6.2;
- CIP-013-AB-2, requirement R3;

6.2. within 14 **days** after the effective date of the CIP Cyber Security **reliability standards** for the following requirement:

- CIP-007-AB-5, requirement R4, Part 4.4;

6.3. within 35 **days** of the Responsible Entity's last performance requirement of requirement R2, Part 2.1 under CIP-010-AB-1:

- CIP-010-AB-4, requirement R2, Part 2.1;

6.4. within 3 **months** after the effective date of the CIP Cyber Security **reliability standards** for the following requirement:

6.5. within 12 **months** after the effective date of the CIP Cyber Security **reliability standards** for the following requirements:

- CIP-006-AB-5, requirement R3, Part 3.1;
- CIP-008-AB-5, requirement R2, Part 2.1;
- CIP-009-AB-5, requirement R2, Parts 2.1 and 2.2; and

6.6. within 15 **months** after the effective date of the CIP Cyber Security **reliability standards** for the following requirements:

- CIP-003-AB-8 R2, Attachment 1, Section 1

6.7. within 15 **months** of the Responsible Entity's last performance requirement of requirement R2, Part 2.3 under CIP-004-AB-5.1

- CIP-004-AB-7, requirement R2, Part 2.3;

6.8. within 15 **months** of the Responsible Entity's last performance requirement of requirement R4, Part 4.3 and 4.4 under CIP-004-AB-5.1

- CIP-004-AB-7, requirement R4, Part 4.3;

6.9. within 15 **months** of the Responsible Entity's last performance requirement of requirement R3, Part 3.1 under CIP-010-AB-1:

- CIP-010-AB-4, requirement R3, Part 3.1; and

6.10. within 24 **months** after the effective date of the CIP Cyber Security **reliability standards** for the following requirements:

- CIP-009-AB-5, requirement R2, Part 2.3; and

6.11. within 36 **months** of the Responsible Entity's last performance requirement of:

- CIP-010-AB-4, requirement R3, Part 3.2

6.12. within 36 **months** after the effective date of the CIP Cyber Security **reliability standards** for the following requirements:

- CIP-003-AB-8, requirement R2, Attachment 1, Section 4.5

7. Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or **BES cyber system** as identified through the annual assessment under CIP-002-AB-5.1, requirement R2, which were planned and implemented by the Responsible Entity identified in the applicability section of each current version of the CIP Cyber Security **reliability standard**.

In contrast, unplanned changes refer to any changes of the electric system or **BES cyber system**, as identified through the annual assessment under CIP-002-AB-5.1, requirement R2, which were not planned by the Responsible Entity identified in the applicability section of each current version of the CIP

Cyber Security **reliability standard**.

For planned changes resulting in a higher categorization, the Responsible Entity identified in the applicability section of each current version of the CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the current version of the CIP Cyber Security **reliability standards** on the update of the identification and categorization of the affected **BES cyber system** and any applicable and associated **physical access control systems**, **electronic access control or monitoring systems** and **protected cyber assets**, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For unplanned changes resulting in a higher categorization, the Responsible Entity identified in the applicability section of each current version of the CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the current version of the CIP Cyber Security **reliability standards**, according to the following timelines, following the identification and categorization of the affected **BES cyber system** and any applicable and associated **physical access control systems**, **electronic access control or monitoring systems** and **protected cyber assets**, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date for Each Version of the CIP Cyber Security Reliability Standard	**Compliance Implementation**
New High Impact **BES cyber system**	12 **months**
New Medium Impact **BES cyber system**	12 **months**
Newly categorized High Impact **BES cyber system** from Medium Impact **BES cyber system**	12 **months** for requirements not applicable to Medium Impact **BES Cyber Systems**
Newly categorized Medium Impact **BES cyber system**	12 **months**
The Responsible Entity identified in the applicability section of each current version of the CIP Cyber Security **reliability standard** identifies first Medium Impact or High Impact **BES cyber system** (i.e., the Responsible Entity identified in the applicability section of each current version of the CIP Cyber Security **reliability standard** previously had no **BES cyber systems** categorized as High Impact or Medium Impact according to the CIP-002-AB-5.1 identification and categorization processes)	24 **months**

For unplanned changes resulting in a low impact categorization where previously the asset containing **BES Cyber Systems** had no categorization, the Responsible Entity shall comply with all requirements applicable to low impact **BES Cyber Systems** within 12 calendar **months** following the identification and categorization of the affected **BES Cyber System**.

Revision History

Effective Date	Description
2024-05-02	Updated to incorporate the adoption of CIP-004-AB-7 AND CIP-011-AB-3; the retirement of CIP-004-AB-5.1 and CIP-011-AB-1; adding effective dates where known. Updated the document to include early compliance option process details for CIP-004-AB-7 and CIP-011-AB-3
2024-10-01	Updated to incorporate the adoption of CIP-003-AB-8, CIP-005-AB-7, CIP-010-AB-4, CIP-013-AB-2; the retirement of CIP-003-AB-5, CIP-005-AB-5, CIP-010-AB-1; added new section General Considerations; updated unplanned changes for low impact categorization; and minor editorial changes, including fixing typographical errors and adding in effective dates where known.
2017-10-01	Initial release