# Alberta Reliability Standard
# Cyber Security – Implementation Plan for Version 5 CIP Security Standards
# CIP-PLAN-AB-1

## 1. Purpose

The purpose of this **reliability standard** is to set the effective dates for the Version 5 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 Version 5 CIP Cyber Security **reliability standards**, which are:

- CIP–002–AB-5.1, *Cyber Security — BES Cyber System Categorization*;
- CIP–003–AB-5, *Cyber Security — Security Management Controls*;
- CIP–004–AB-5.1, *Cyber Security — Personnel and Training*;
- CIP–005–AB-5, *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-1, *Cyber Security — Configuration Change Management and Vulnerability Assessments*; and
- CIP–011–AB-1, *Cyber Security — Information Protection*.

## 3. Compliance with Reliability Standards

Once the Version 5 CIP Cyber Security **reliability standards** become effective, the "Responsible Entities" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** must comply with the requirements of those **reliability standards**.

## 4. Proposed Effective Date

The Version 5 Cyber Security **reliability standards**, except for requirement R2 of CIP-003-AB-5, become effective on the first **day** of the calendar quarter (January 1, April 1, July 1 or October 1) that follows eight (8) full calendar quarters after approval by the **Commission**. Requirement R2 of CIP-003-AB-5 becomes effective on the first **day** of the calendar quarter (January 1, April 1, July 1 or October 1) that follows twelve (12) full calendar quarters after approval by the **Commission**.

## 5. Initial Performance of Certain Periodic Requirements

Specific Version 5 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 fifteen (15) **months** . . .", and "Responsible Entities" must comply initially with those periodic requirements as follows:

1. on or before the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:

- CIP-002-5, requirement R2; and
- CIP-003-5, requirement R1;

2. on or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, requirement R2;
3. within fourteen (14) **days** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirement:
   - CIP-007-5, requirement R4, Part 4.4;
4. within thirty-five (35) **days** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-010-1, requirement R2, Part 2.1;
5. within three (3) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirement:
   - CIP-004-5, requirement R4, Part 4.2;
6. within twelve (12) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-004-5, requirement R2, Part 2.3;
   - CIP-004-5, requirement R4, Parts 4.3 and 4.4;
   - CIP-006-5, requirement R3, Part 3.1;
   - CIP-008-5, requirement R2, Part 2.1;
   - CIP-009-5, requirement R2, Parts 2.1 and 2.2; and
   - CIP-010-1, requirement R3, Part 3.1; and
7. within twenty-four (24) **months** after the effective date of the Version 5 CIP Cyber Security **reliability standards** for the following requirements:
   - CIP-009-5, requirement R2, Part 2.3; and
   - CIP-010-1, requirement R3, Part 3.2.

## 6. 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 Version 5 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 Version 5 CIP Cyber Security **reliability standard**.

For planned changes resulting in a higher categorization, the "Responsible Entity" identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the Version 5 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 Version 5 CIP Cyber Security **reliability standard** shall comply with all applicable requirements in the Version 5 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 5 CIP Cyber Security Reliability Standard | Compliance Implementation |
|---|---|
| New High Impact **BES cyber system** | twelve (12) **months** |
| New Medium Impact **BES cyber system** | twelve (12) **months** |
| Newly categorized High Impact **BES cyber system** from Medium Impact **BES cyber system** | twelve (12) **months** for requirements not applicable to Medium Impact **BES Cyber Systems** |
| Newly categorized Medium Impact **BES cyber system** | twelve (12) **months** |
| The "Responsible Entity" identified in the applicability section of each Version 5 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 Version 5 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) | twenty-four (24) **months** |

## Revision History

| Date | Description |
|---|---|
| 2017-10-01 | Initial release. |