Alberta Reliability Standard
Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-010-AB-4

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-AB-4

3. Purpose: To prevent and detect unauthorized changes to **BES cyber systems** ~~BES Cyber Systems~~ by specifying configuration change management and vulnerability assessment requirements in support of protecting **BES cyber systems** ~~BES Cyber Systems~~ from compromise that could lead to misoperation or instability in the **bulk electric system** ~~Bulk Electric System (BES)~~.

4. Applicability:

4.1. Functional Entities**:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. [Intentionally left blank.] ~~**Balancing Authority**~~

4.1.2. a **legal owner** of an **electric distribution system** ~~**Distribution Provider**~~ that owns one or more of the following facilities ~~Facilities~~, systems, and equipment for the protection or restoration of the **bulk electric system** ~~BES~~:

4.1.2.1. Each **underfrequency load shedding** ~~underfrequency Load shedding (UFLS)~~ or **under voltage load shed** ~~undervoltage Load shedding (UVLS)~~ system that:

4.1.2.1.1. is part of a load ~~Load~~ shedding program that is subject to one or more requirements in a **reliability standard** ~~NERC or Regional Reliability Standard~~; and

4.1.2.1.2. performs automatic ~~Load~~ load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more; ~~.~~

4.1.2.2. Each **remedial action scheme** ~~Remedial Action Scheme (RAS)~~ where the **remedial action scheme** ~~RAS~~ is subject to one or more requirements in a **reliability standard;** ~~NERC or Regional Reliability Standard.~~

4.1.2.3. Each **protection system** ~~Protection System~~ (excluding **underfrequency load shedding** ~~UFLS~~ and **under voltage load shed** ~~UVLS~~) that applies to ~~Transmission~~ any **electric distribution system** where the **protection system** ~~Protection System~~ is subject to one or more requirements in a **reliability standard** ~~NERC or Regional Reliability Standard.~~ ; and

4.1.2.4. Each **cranking path** ~~Cranking Path~~ and group of ~~Elements~~ elements meeting the initial switching requirements from a **blackstart resource** ~~Blackstart Resource~~ up to and including the first **point of connection** ~~interconnection point~~ of the starting station service of the next **generating unit**(s) or **aggregated generating facility**(ies) ~~generation unit(s)~~ to be started.

4.1.3. the **operator** of a **generating unit** that is part of the **bulk electric system** and the **operator** of an **aggregated generating facility** that is part of the **bulk electric system**; ~~**Generator Operator**~~

4.1.4. the **legal owner** of a **generating unit** that is part of the **bulk electric system** and the **legal owner** of an **aggregated generating facility** that is part of the **bulk electric system**;~~**Generator Owner**~~

4.1.5. [Intentionally left blank.]~~**Reliability Coordinator**~~

4.1.6. the **operator** of a **transmission facility**;~~**Transmission Operator**~~

4.1.7. the **legal owner** of a **transmission facility**; and~~**Transmission Owner**~~

4.1.8. the **ISO.**

4.2. Facilities**:** For the purpose of the requirements contained herein, the following ~~Facilities~~facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this **reliability standard** ~~standard~~ where a specific type of ~~Facilities~~facilities, system, or equipment or subset of ~~Facilities~~facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Legal owner of an **electric distribution system** and **legal owner** of a **transmission facility**;~~**Distribution Provider**~~**:** One or more of the following ~~Facilities~~facilities, systems and equipment that operate at, or control elements that operate at, a nominal voltage of 25 kV or less and are owned by a **legal owner** of an **electric distribution system** or a **legal owner** of a **transmission facility** ~~the Distribution Provider~~ for the protection or restoration of the **bulk electric system** ~~BES~~:

4.2.1.1. Each **underfrequency load shedding** ~~UFLS~~ or **under voltage load shed**~~UVLS System~~ system that:

4.2.1.1.1. is part of a ~~Load~~ load shedding program that is subject to one or more requirements in a **reliability standard**~~NERC or Regional Reliability Standard~~; and

4.2.1.1.2. performs automatic ~~Load~~ load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each **remedial action scheme** ~~RAS~~ where the **remedial action scheme** ~~RAS~~ is subject to one or more requirements in a **reliability standard**~~NERC or Regional Reliability Standard~~.

4.2.1.3. Each **protection system** ~~Protection System~~ (excluding **underfrequency load shedding** ~~UFLS~~ and **under voltage load shed**~~UVLS~~) that applies to any **transmission facility** or **electric distribution system**~~Transmission~~ where the **protection system** ~~Protection System~~ is subject to one or more requirements in a **reliability standard**~~NERC or Regional Reliability Standard~~.

4.2.1.4. Each **cranking path** ~~Cranking Path~~ and group of ~~Elements~~ elements meeting the initial switching requirements from a **blackstart resource**~~Blackstart Resource~~ up to and including the first **point of connection**~~interconnection point~~ of the starting station service of the next **generating unit**(s) or **aggregated generating facility**(ies)~~generation unit(s~~) to be started.

4.2.2. Responsible Entities listed in 4.1 other than a **legal owner** of an **electric distribution system** ~~**Distribution Providers**~~**:**

all **bulk electric system** facilities~~All BES Facilities~~.

4.2.3. Exemptions: The following are exempt from ~~Standard~~ CIP-010-AB-4:

4.2.3.1. **Cyber assets**~~Cyber Assets~~ at facilities~~Facilities~~ regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. **Cyber assets** ~~Cyber Assets~~ associated with communication networks and data communication links between discrete **electronic security perimeters**~~Electronic Security Perimeters~~.

4.2.3.3. [Intentionally left blank.]~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54~~.

4.2.3.4. For the **legal owner** of an **electric distribution system**~~Distribution Providers~~, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no **BES cyber systems** ~~BES Cyber Systems~~ categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates: ~~See Implementation Plan for Project 2019-03~~ *To be determined in consultation with stakeholders*.

6. Background:

Reliability standard~~Standard~~ CIP-010 exists as part of a suite of CIP **reliability standards**~~Standards~~ related to cyber security, which require the initial identification and categorization of **BES cyber systems** ~~BES Cyber Systems~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to **BES cyber systems**~~BES Cyber Systems~~.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact **BES cyber systems**~~BES Cyber Systems~~. For example, a single training program could meet the requirements for training personnel across multiple **BES cyber systems**~~BES Cyber Systems~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for **underfrequency load shedding** ~~UFLS~~ and **under voltage load shed**~~UVLS~~. This particular threshold of 300 MW for **under voltage load shed** ~~UVLS~~ and **underfrequency load shedding** ~~UFLS~~ was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing **under voltage load shed** ~~UVLS~~ and **underfrequency load shedding**~~UFLS~~, which are last ditch efforts to save the Bulk Electric System. A review of **underfrequency load shedding** ~~UFLS~~ tolerances defined within **reliability standards**~~regional reliability standards~~ for **underfrequency load shedding** ~~UFLS~~ program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable **underfrequency load shedding** ~~UFLS~~ operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 NERC standard drafting team~~SDT~~ adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to **BES cyber systems**~~BES Cyber Systems~~ categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to **BES cyber systems**~~BES Cyber Systems~~ categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems ~~(EACMS)~~** – Applies to each **electronic access control or monitoring system**~~Electronic Access Control or Monitoring System~~ associated with a referenced high impact **BES cyber system**~~BES Cyber System~~ or medium impact **BES cyber system**~~BES Cyber System~~. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems ~~(PACS)~~** – Applies to each **physical access control system**~~Physical Access Control System~~ associated with a referenced high impact **BES cyber system**~~BES Cyber System~~ or medium impact **BES cyber system**~~BES Cyber System~~.
- **Protected Cyber Assets ~~(PCA)~~** – Applies to each **protected cyber asset**~~Protected Cyber Asset~~ associated with a referenced high impact **BES cyber system**~~BES Cyber System~~ or medium impact **BES cyber system**~~BES Cyber System~~.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-AB-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Commented AESO: **Difference since CIP-010-AB-1:**
Removed "identify, asses, correct" language.

Original wording:
Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R1 – Configuration Change Management*.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each **cyber asset**~~Cyber Asset~~, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each **cyber asset**~~Cyber Asset~~, individually or by group.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 **days**~~calendar days~~ of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 **days**~~calendar days~~ of the date of the completion of the change.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact **BES cyber systems**~~BES Cyber Systems~~	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

1.6	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; and 2. **physical access control systems**~~PACS~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; and 2. **physical access control systems**~~PACS~~ Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

Commented AESO: **Difference since CIP-010-AB-1:**
New requirement R1.6

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	contract.		

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-AB-4 Table R2 – Configuration Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Commented AESO: Difference since CIP-010-AB-1:
Removed "identify, asses, correct" language.

Original wording:
Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R2 – Configuration Monitoring*

CIP-010-AB-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** ~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems** ~~EACMS~~; and 2. **protected cyber assets** ~~PCA~~	Monitor at least once every 35 **days** ~~calendar days~~ for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-AB-43 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-43 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-AB-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	At least once every 15 **months**~~calendar months~~, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 **months**~~calendar months~~), the controls assessed for each **BES cyber system**~~BES Cyber System~~ along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-AB-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact **BES cyber systems**~~BES Cyber Systems~~	Where technically feasible, at least once every 36 **months**~~calendar months~~: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the **BES cyber system**~~BES Cyber System~~ in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 **months**~~calendar months~~), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-AB-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; and 2. **protected cyber assets**~~PCA~~	Prior to adding a new applicable **cyber asset**~~Cyber Asset~~ to a production environment, perform an active vulnerability assessment of the new **cyber asset**~~Cyber Asset~~, except for **CIP exceptional circumstances**~~CIP Exceptional Circumstances~~ and like replacements of the same type of **cyber asset**~~Cyber Asset~~ with a baseline configuration that models an existing baseline configuration of the previous or other existing **cyber asset**~~Cyber Asset~~.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new **cyber asset**~~Cyber Asset~~) and the output of any tools used to perform the assessment.

CIP-010-AB-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact **BES cyber systems**~~BES Cyber Systems~~ and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~; 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~ Medium Impact ~~BES Cyber Systems~~**BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**~~EACMS~~ 2. **physical access control systems**~~PACS~~; and 3. **protected cyber assets**~~PCA~~	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact **BES cyber systems**~~BES Cyber Systems~~ and associated **protected cyber assets**~~Protected Cyber Assets~~, shall implement, except under **CIP exceptional circumstances**~~CIP Exceptional Circumstances~~, one or more documented plan(s) for transient cyber assets~~Transient Cyber Assets~~ and removable media~~Removable Media~~ that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for transient cyber assets~~Transient Cyber Assets~~ and removable media~~Removable Media~~ that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for transient cyber assets~~Transient Cyber Assets~~ and removable media~~Removable Media~~. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use transient cyber asset(s)~~Transient Cyber Asset(s)~~ or removable media~~Removable~~

Commented AESO: **Difference since CIP-010-AB-1:** New requirement R4. References new Attachment 1 and Attachment 2.

Commented AESO: "Transient Cyber Assets" and "Removable Media" will be considered for addition to the AESO CADG. Proposed definitions are available in the concordance document.

~~Media~~, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use transient cyber asset(s)~~Transient Cyber Asset(s)~~ or removable media~~Removable Media~~.

C. Compliance

[Intentionally left blank.]

~~**1. Compliance Monitoring Process**~~

~~**1.1. Compliance Enforcement Authority:**~~

~~"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.~~

~~**1.2. Evidence Retention:**~~

~~The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.~~

~~The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.~~

~~• Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.~~

~~• If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.~~

~~• The CEA shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~**1.3. Compliance Monitoring and Enforcement Program:**~~

~~As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

Violation Severity Levels

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration. (1.3) OR

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP- 007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-4, Requirement R4, Attachment 1, Section 3. (R4)	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-4, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-4, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-4, Requirement R4. (R4)

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Section 1.2. (R4)	Cyber Assets managed by the Responsible Entity according to CIP-010- 4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Cyber Assets managed by the Responsible Entity according to CIP-010- 4, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-4, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

~~• Implementation Plan for Project 2019-03~~

• CIP-010-4 Technical Rationale

Version History

Version	~~Effective~~ Date	~~Action~~	Change Tracking
~~1~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.~~
1	~~11/22/13~~ 10/1/2017	~~FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)~~	Initial Version
~~2~~	~~11/13/14~~	~~Adopted by the NERC Board of Trustees.~~	~~Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.~~

Version	Effective Date	Action	Change Tracking
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021TBD	Effective Date	10/1/2022 Aligns with NERC changes which: addressed FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks, as well as transient devices and low impact BES cyber systems. Also modified to address FERC Order No. 829 and 850.

CIP-010-AB-4 - Attachment 1

Commented AESO: **Difference since CIP-010-AB-1:** New Attachment 1 per R4

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for transient cyber assets~~Transient Cyber Assets~~ and removable media~~Removable Media~~ as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage transient cyber asset(s)~~Transient Cyber Asset(s)~~, individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a **BES cyber system**~~BES Cyber System~~, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of transient cyber asset(s)~~Transient Cyber Asset(s)~~, each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the transient cyber asset~~Transient Cyber Asset~~ (per transient cyber asset~~Transient Cyber Asset~~ capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per transient cyber asset~~Transient Cyber Asset~~ capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of transient cyber

asset(s)~~Transient Cyber Asset(s)~~:

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the transient cyber asset~~Transient Cyber Asset~~ (per transient cyber asset~~Transient Cyber Asset~~ capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per transient cyber asset~~Transient Cyber Asset~~ capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the transient cyber asset~~Transient Cyber Asset~~.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of removable media~~Removable Media~~, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact **BES cyber systems**~~BES Cyber Systems~~ and their associated **protected cyber assets**~~Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on removable media~~Removable Media~~ using a **cyber asset**~~Cyber Asset~~ other than a **BES cyber system**~~BES Cyber System~~ or **protected cyber assets**~~Protected Cyber Assets~~; and

3.2.2. Mitigate the threat of detected malicious code on removable media~~Removable Media~~ prior to connecting the removable media~~Removable Media~~ to a high impact or medium impact **BES cyber system**~~BES Cyber System~~ or associated **protected cyber assets**~~Protected Cyber Assets~~.

CIP-010-AB-4 - Attachment 2

Commented AESO: **Difference since CIP-010-AB-1:** New Attachment 2 per R4

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the transient cyber asset(s)~~Transient Cyber Asset(s)~~. This can be included as part of the transient cyber asset~~Transient Cyber Asset~~ plan(s), part of the documentation related to authorization of transient cyber asset(s)~~Transient Cyber Asset(s)~~ managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of transient cyber asset(s)~~Transient Cyber Asset(s)~~ managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a transient cyber asset~~Transient Cyber Asset~~ does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the transient cyber asset~~Transient Cyber Asset~~ does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a transient cyber asset~~Transient Cyber Asset~~ does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the transient cyber asset~~Transient Cyber Asset~~ does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the

security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for transient cyber asset(s)~~Transient Cyber Asset(s)~~ managed by a party other than the Responsible Entity. If a transient cyber asset~~Transient Cyber Asset~~ does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the transient cyber asset~~Transient Cyber Asset~~ does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for transient cyber asset(s)~~Transient Cyber Asset(s)~~ managed by a party other than the Responsible Entity. If a transient cyber asset~~Transient Cyber Asset~~ does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the transient cyber asset~~Transient Cyber Asset~~ does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the transient cyber asset~~Transient Cyber Asset~~ managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of removable media~~Removable Media~~. The documentation must identify removable media~~Removable Media~~, individually or by group of removable media~~Removable Media~~, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for removable media~~Removable Media~~, or implementation of on- demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on removable media~~Removable Media~~, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on removable media~~Removable Media~~ or documented confirmation by the entity that the removable media~~Removable Media~~

was deemed to be free of malicious code.