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** by specifying configuration change management and vulnerability assessment requirements in support of protecting **BES cyber systems** from compromise that could lead to misoperation or instability in the **bulk electric system**.

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 **reliability 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.]

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

4.1.2.1. Each **underfrequency load shedding** or **under voltage load shed** system that:

4.1.2.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.1.2.1.2. performs automatic 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** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard;**

4.1.2.3. Each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to an **electric distribution system** where the **protection system** is subject to one or more requirements in a **reliability standard**; and

4.1.2.4. Each **cranking path** and group of elements meeting the initial switching requirements from a **blackstart resource** up to and including the first **point of connection** of the starting station service of the next **generating unit**(s) or **aggregated generating facility**(ies) 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**;

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**;

4.1.5. [Intentionally left blank.]

4.1.6. the **operator** of a **transmission facility**;

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

4.1.8. the **ISO**.

4.2. Facilities**:** For the purpose of the requirements contained herein, the following 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** where a specific type of facilities, system, or equipment or subset of 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:** One or more of the following 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** for the protection or restoration of the **bulk electric system**:

4.2.1.1. Each **underfrequency load shedding** or **under voltage load shed** system that:

4.2.1.1.1. is part of a load shedding program that is subject to one or more requirements in a **reliability standard**; and

4.2.1.1.2. performs automatic 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** where the **remedial action scheme** is subject to one or more requirements in a **reliability standard**.

4.2.1.3. Each **protection system** (excluding **underfrequency load shedding** and **under voltage load shed**) that applies to any **transmission facility** or **electric distribution system** where the **protection system** is subject to one or more requirements in a **reliability standard**.

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

4.2.2. Responsible Entities listed in 4.1 other than a **legal owner** of an **electric distribution system:** all **bulk electric system** facilities.

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

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

4.2.3.2. **Cyber assets** associated with communication networks and data communication links between discrete **electronic security perimeters**.

4.2.3.3. [Intentionally left blank.].

4.2.3.4. For the **legal owner** of an **electric distribution system**, 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** categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. Effective Dates: See CIP-PLAN-AB-2, *Cyber Security – Implementation Plan for CIP Cyber Security Reliability Standards*

6. Background:

Reliability standard CIP-010 exists as part of a suite of CIP **reliability standards** related to cyber security, which require the initial identification and categorization of **BES cyber systems** and require a minimum level of organizational, operational and procedural controls to mitigate risk to **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 **reliability standards** include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security **reliability 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 **reliability standards**.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact **BES cyber systems**. For example, a single training program could meet the requirements for training personnel across multiple **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 **reliability 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** and **under voltage load shed**. This particular threshold of 300 MW for **under voltage load shed** and **underfrequency load shedding** was provided in the NERC Version 1 of the CIP Cyber Security reliability standards. The threshold remains at 300 MW since it is specifically addressing **under voltage load shed** and **underfrequency load shedding**, which are last ditch efforts to save the Bulk Electric System. A review of **underfrequency load shedding** tolerances defined within **reliability standards** for **underfrequency load shedding** program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable **underfrequency load shedding** 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 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** categorized as high impact according to the CIP-002 identification and categorization processes.
- Medium Impact **BES Cyber Systems** – Applies to **BES cyber systems** categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems** – Applies to each **electronic access control or monitoring system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems** – Applies to each **physical access control system** associated with a referenced high impact **BES cyber system** or medium impact **BES cyber system**.
- **Protected Cyber Assets** – Applies to each **protected cyber asset** associated with a referenced high impact **BES cyber system** or medium impact **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*. *[Alberta Risk Rating: 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.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	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**, 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**, 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** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	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** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 **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** 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** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	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**	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.

CIP-010-AB-4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **physical access control systems** 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 contract.	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.

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*. *[Alberta Risk Rating: 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.

CIP-010-AB-4 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Monitor at least once every 35 **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-4 Table R3– Vulnerability Assessments*. *[Alberta Risk Rating: 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-4 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** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	At least once every 15 **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**), the controls assessed for each **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**	Where technically feasible, at least once every 36 **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** 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**), 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** and their associated: 1. **electronic access control or monitoring systems**; and 2. **protected cyber assets**	Prior to adding a new applicable **cyber asset** to a production environment, perform an active vulnerability assessment of the new **cyber asset**, except for **CIP exceptional circumstances** and like replacements of the same type of **cyber asset** with a baseline configuration that models an existing baseline configuration of the previous or other existing **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**) and the output of any tools used to perform the assessment.
3.4	High Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems**; 2. **physical access control systems**; and 3. **protected cyber assets** Medium Impact **BES cyber systems** and their associated: 1. **electronic access control or monitoring systems** 2. **physical access control systems**; and 3. **protected cyber assets**	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** and associated **protected cyber assets**, shall implement, except under **CIP exceptional circumstances**, one or more documented plan(s) for **transient cyber assets** and **removable media** that include the sections in Attachment 1. *[Alberta Risk Rating: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for **transient cyber assets** and **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** and **removable media**. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use **transient cyber asset**(s) or **removable 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) or **removable media**.

C. Compliance

[Intentionally left blank.]

D. Regional Variances

None.

E. Associated Documents

- CIP-PLAN-AB-2, *Cyber Security – Implementation Plan for CIP Cyber Security Reliability Standards*
- NERC *Cyber Security - Configuration Change Management and Vulnerability Assessments: Technical Rationale and Justification for Reliability Standard CIP-010-4*
- AESO Information Document, #2015-003RS, *Guidance Information for CIP Standards* and any amendments made thereto from time to time.

Version History

Version	Effective Date	Description of Changes
1	10/1/2017	Initial Version
4	10/1/2024	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

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** and **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), 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**, 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), 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** (per **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** capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application allowlisting; 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):

- 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** (per **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** capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application allowlisting 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**.

Section 3. **Removable Media**

3.1. **Removable Media** Authorization: For each individual or group of **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** and their associated **protected cyber assets**, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on **removable media** using a **cyber asset** other than a **BES cyber system** or **protected cyber assets**; and

3.2.2. Mitigate the threat of detected malicious code on **removable media** prior to connecting the **removable media** to a high impact or medium impact **BES cyber system** or associated **protected cyber assets**.

CIP-010-AB-4 - Attachment 2

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). This can be included as part of the **transient cyber asset** plan(s), part of the documentation related to authorization of **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) 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** 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** 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 allowlisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a **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** 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) managed by a party other than the Responsible Entity. If **a 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** 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 allowlisting, 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) managed by a party other than the Responsible Entity. If a **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** 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** 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**. The documentation must identify **removable media**, individually or by group of **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**, 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**, 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** or documented confirmation by the entity that the **removable media** was deemed to be free of malicious code.