A. Introduction

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

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the 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. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional 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 (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   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 interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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 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. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional 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 RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional 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 interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. 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.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. 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.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 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-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not	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, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		adversely affected; and 1.2.2. 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.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. 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 the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. 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 installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 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-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 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-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 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 calendar 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-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; 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 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.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	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.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation 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, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and 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 TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(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 TCA(s) or Removable Media.

C. Compliance

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 #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required	The Responsible Entity neither documented nor implemented a configuration monitoring process(es); or the process does not include five or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable 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. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not 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 Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-010-5 Technical Rationale

Version History

Version	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	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
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.
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	4/5/2021	Effective Date	10/1/2022
5			Virtualization Modifications under Project 2016-02
5	5/9/2024	Approved by the NERC Board of Trustees.	

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. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(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, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(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 TCA (per TCA capability):

- Security patching, including manual or managed updates;
- 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 risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; 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 TCA(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. TCA(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 TCA (per TCA 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
- Review of 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 the risk of introduction of malicious code (per TCA 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
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used 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 TCA.

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, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - 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 TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(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 TCA(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 the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of 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, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA 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 TCA 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 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 TCA 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; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; 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 TCA(s) managed by a party other than the Responsible Entity. If a TCA 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 TCA 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, and system hardening 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 TCA(s) managed by a party other than the Responsible Entity. If a TCA 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 TCA 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 TCA 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.