The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

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

2. **Number:** CIP-010-4~~3~~

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability ~~assessment~~ management requirements in support of protecting BES Cyber Systems 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 in this standard~~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 explicitly 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.~~4.1.4. ~~Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For ~~the purpose of~~ the requirements ~~contained herein~~in this standard, 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, systems, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly 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-010-4~~3~~:

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~~-~~ BES Cyber Systems' Logical Isolation Zones (LIZ).~~discrete Electronic Security Perimeters~~.

~~4.2.3.2.~~4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~4.2.3.3.~~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.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~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-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for ~~Project 2016-03~~CIP-010-4.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by insecure system configuration that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 4 Table R1 – Secure Configuration ~~Change~~ Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.1~~	~~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~~	~~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:~~ ~~• Documentation A spreadsheet identifying the required items of the baseline secure configuration for each Cyber Assetsystem, 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.~~

1.1~~2~~	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Control change to the S~~s~~ecure C~~c~~onfiguration ~~described in CIP-010 Requirement R1 Part 1.1~~ implemented on systems through: ~~Authorize and document changes that deviate from the existing baseline configuration.~~ ~~1.1.1.~~ 1.1.1. Authorization; 1.1.2. Prior to the change, determine required cyber security controls in the Secure Configuration that could be impacted by the change; 1.1.3. Implementation; and 1.1.4. Following the change, verify that required cyber security ~~controls determined~~controls determined in 1.1.2 are not adversely affected~~;~~ and document the results. ~~.~~ The process requirements of Parts 1.1.1 through 1.1.4 and timeline are based on the analysis of the risk to BES reliability and the risk posed by the change to the system(s).	Examples of evidence may include, but are not limited to: • ~~A change request record and~~ R~~r~~ecords ~~for~~of authorization~~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~~ • Records of ~~testing~~controls impact ~~evaluaton~~evaluation; • Records of implementation; and • Records of ~~evaluation~~verification. ~~Documentation that the change was performed in accordance with the requirement.~~

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 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 calendar days of the date of the completion of the change.~~
~~1.4~~	~~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~~	~~For a change that deviates from the existing baseline configuration:~~ ~~Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~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.~~

1.2~~5~~	High Impact BES Cyber Systems	~~Where technically feasible, f~~For each change that deviates from the ~~existing baseline~~ implemented Secure C~~c~~onfiguration, perform the following, per system capability, except during CIP Exceptional Circumstances: 1.2.1. Prior to implementing any change in the production environment, test the changes in a test environment; or ~~-~~test the changes ~~test the changes~~ in a production environment where the test is performed in a manner that minimizes adverse effects, that models the ~~baseline~~ Secure C~~c~~onfiguration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.~~2~~2.~~3~~ Document the results of the testing and,~~.~~ ~~and, i~~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	An example of evidence may include, but is not limited to, a list of tested cyber security controls, test dates, ~~tested along with~~ successful test results, and ~~and~~ a list of differences between the production and test environments including ~~with~~ descriptions of how any differences in the test and production environments were ~~addressed.~~accounted for ~~how any differences were accounted for~~.~~,~~ ~~including of the date of the test.~~

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		between the test and production environments.	
1.3~~6~~	High Impact BES Cyber Systems Medium Impact BES Cyber 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 1.3~~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~~ Secure C~~c~~onfiguration associated with installing or updating ~~baseline CIP-007-7 R2 and CIP-010-4 R3 Part 3~~operating system, firmware, and software~~.6secure configuration 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: 1.3~~6~~.1. Verify the identity of the software source; and 1.3~~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~~ Secure Configuration 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) to mitigate the risk posed by unauthorized change to Secure Configurations that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R2 – Secure Configuration Monitoring*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R2 – Secure Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~ 4Table R2 – Secure Configuration ~~Monitoring~~

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Use one or a combination of the following methods to monitor the implemented Secure Configuration (per system capability): ~~Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.~~ • Hash monitoring; • Configuration monitoring; • Configuration auditing; or • Other method(s) to mitigate the risk posed by unauthorized change to Secure Configurations. The process requirements of Part 2.1 and timeline are based on the analysis of the risk to BES reliability and the impact rating of the applicable system(s).	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.
2.2	High Impact BES Cyber Systems and their associated:	Investigate and remediate detected unauthorized changes to the	An example of evidence may include, but is not limited to, records of

CIP-010-~~3~~ 4Table R2 – Secure Configuration ~~Monitoring~~

Part	Applicable Systems	Requirements	Measures
	1. EACS; and 2. PCS	implemented Secure Configuration found through implementation of Requirement R2 Part 2.1. The process requirements of Part 2.2 and timeline are based on the analysis of the risks to BES reliability and the risks posed by the detected unauthorized change to the implemented Secure Configuration	unauthorized change investigations and remediating activities.

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by system vulnerabilities that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R3– Vulnerability ~~Assessments~~Management*.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~ Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	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-~~4~~3 Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	~~Where technically feasible,~~ Per system capability, at least once every 36 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~~ Secure C~~c~~onfiguration 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 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-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management

Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PCS~~A~~	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 and additions of the same type of Cyber Asset with a ~~baseline~~ Secure C~~c~~onfiguration that models an existing ~~baseline~~ Secure C~~c~~onfiguration 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~~-~~ addition~~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. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	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).

CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management

Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify software vulnerabilities using one or more of the following methods: • Vulnerability database monitoring; • Patch source monitoring; • Vulnerability scanning; or • Other method(s) to identify software vulnerabilities. The process of Part 3.5 shall include the periodicity for identifying software vulnerabilities based on the risk to BES reliability and the impact rating of the applicable system(s).	An example of evidence may include, but is not limited to: • Records of vulnerability database monitoring; • Records of patch source monitoring; or • Records of vulnerability scanning.

CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management			
Part	Applicable Systems	Requirements	Measures
3.6	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Create or update a plan to mitigate the identified software vulnerabilities from Part 3.5, through one or more of the following: • Implementing security patches; • Applying compensating controls; • System hardening; or • Other method(s) to mitigate software vulnerabilities. The plan for Part 3.6 must include the timeline for mitigating the software vulnerability based on the analysis of the risk posed by the software vulnerability to the applicable systems. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to: • Records of implemented security patches; • Records of applied compensating controls; • Records of system hardening; or • Records of other methods.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber ~~Assets~~Systems, 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.

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

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" 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 Compliance Enforcement Authority 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 Compliance Enforcement Authority 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.

D. Regional Variances

None.

E. Associated Documents

None.

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

Version	Date	Action	Change Tracking
			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.	

CIP-010-4~~3~~ - 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 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):

- 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 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.

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~~System, 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~~System; 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~~System.

CIP-010-4~~3~~ - 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 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 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 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) 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.