NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference.

Virtualization Concepts Driving CIP-010 Changes

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Where entries elect to utilize "Shared Cyber Infrastructure", virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow the hardware infrastructure to be shared among several Virtual Cyber Assets (VCAs) that may be of differing impact levels. Hypervisors must include security controls to keep these workloads logically isolated from one another and those requirements are within other CIP standards such as CIP-005 and CIP-007. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

As discussed elsewhere, entities may choose to high watermark all VCAs executing in their virtualized infrastructure, known as the "all-in" scenario, and not be concerned with SCI specific requirements. They simply consider the underlay part of the highest impact BCS VCA executing on it and comply with the appropriate security controls and requirements for it.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a Cyber Asset or VCA can be isolated from having routable connectivity to any BES Cyber Systems (typically only having visibility of remediation services such as patching and antimalware updates, etc.) while it is examined to ensure the integrity and validity of the configuration and software installed on it. After this examination and subsequent remediation of deficiencies is completed, it is then joined to its production network.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for a successful examination. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the asset, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the asset may communicate the deficiencies to the asset with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the asset can request to be re-examined and if the requirements dictated by the policy are now met, it will be joined to its production network.

Parent/Child Images

When a VCA is 'powered on' or begins execution, it instantiates ("boots") from a disk image file. Since the boot 'disk' is a file and not physical disk, many individual VCAs can use the same "parent" image as the basis for their own "child" image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation. A common use of parent/child images is Virtual Desktop Infrastructures (VDI) that deliver a temporary desktop environment to each remote user for the duration of their session that are VCAs instantiated from a parent image.

Dormant VMs

A VCA that is not currently executing or instantiated (i.e., not 'booted up') is a dormant VM. It exists not as a traditional VCA, but simply as a file. VCA's can be created for specialized purposes such as to run troubleshooting tools and are only instantiated when needed and may be dormant for long periods of time. They are not instantiated and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do begin to instantiate.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added "SCI that supports an Applicable System in this Part." This approach keeps the SCI applicability parallel to each existing variant of Medium Impact BCS (i.e., Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS or firmware, installed and custom software, ports, and patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on maintaining documentation of past changes. However, in CIP-010-4 the core security objective of R1 was in Part 1.2 to authorize and document changes and the baseline configuration was used primarily to set the scope of those changes. Maintaining the baseline configuration information within 30 days after making changes is not a security objective, and as we implement more dynamic systems and more automation of change with virtualization, it becomes more problematic.

In CIP-010-5, the SDT considered the more dynamic, policy-based, and automated virtualization technologies discussed in the previous section and determined to focus Requirement R1 on the true security objective of change management and authorizing intended changes. In other words, make R1.2 from version 4 the main focal point in version 5. Maintaining documentation of ever more automated updates to systems after the fact gives way in this version to authorizing changes that will affect the security posture of the system. The SDT is addressing VCA's that may be dormant for long periods of time and dynamically patched at a future instantiation when needed. The SDT considered the focus of R1 is not for entities to track the date/time a VCA may be dynamically instantiated and patched in an automated fashion in a remediation VLAN and then provide evidence that a baseline configuration was updated within 35 days of that dynamic event.

In addition, with the introduction of application containers and orchestration (Kubernetes, Docker Swarms, etc.), application software may no longer be "installed" on a particular OS instance on a particular server. Instead, an orchestration service may instantiate an application container on the best "node" (server with container runtime) at the moment. For example, a dedicated "database server" gives way to a "database service" that can be instantiated in a container on any VCA or CA managed by the orchestrator. Therefore, baseline configurations of statically installed software and open ports loses value as it becomes dynamically managed in these scenarios. The focus of R1 has thus changed from documenting how the VCA is configured at some point post-change to authorizing the changes that will occur to it when it does instantiate, which provides more security value.

Entities may of course continue to maintain and use baseline configurations, but in CIP-010-5 it is no longer the singular prescribed way of setting change management scope and documenting changes. Baseline configurations may continue to be used as evidence for CIP-007 R1 for example, documenting the enabled ports on a system. In fact, baseline configurations will probably continue to be a very common method used by entities to help detect unauthorized changes in CIP-010 R2, but the standard does not prescribe it as the singular way to meet these security objectives. Therefore, the phrase "baseline configuration" has been removed from CIP-010-5 though entities may continue using it as their "how". Again, the focus of R1 in CIP-010-4 and CIP-010-5 is authorizing changes that affect the security posture of the applicable systems; the SDT has just brough it forward as the "what" with baseline configurations as one possible, but not prescribed, "how". Entities may also wish to reference NIST SP 800-128 "Guide for Security-Focused Configuration Management of Information Systems" as a guide for additional information.

The SDT also considered at length the scope of changes that should be subject to R1. In CIP-010-4, the scope was set by the prescribed elements in the baseline config, consisting essentially of software, patches, and ports. As mentioned above, the security objective of putting ports in the baseline configuration is not to document and maintain a list of listening ports; that security objective is covered in CIP-007 R1 to reduce the attack surface by disabling unneeded ports. Maintaining documentation of the patches installed on a system (which becomes more problematic over time with vendor-bundled monthly updates that may install/remove patches differently per each system's needs) is not the security objective. Knowing what patches are available and applicable to the systems and installing them and mitigating the risk is the goal as covered in CIP-007 R2. In CIP-010 R1, authorizing the action in order to manage change is the objective.

In addition, the SDT considered the prescribed list of baseline configuration elements was insufficient as the scope of a change management requirement. For example, in an SCI that is configured to isolate VCAs of different impact levels from each other, managing and authorizing change to that configuration is vital. As Zero Trust architectures come to fruition, managing and authorizing changes to those access policies is crucial. These are all very important security configurations that were not enumerated in CIP-010-4's baseline configuration and thus not in scope. The SDT concluded that creating a longer prescriptive list of items was not appropriate, in that such a list would need to be maintained as technology changes. The SDT decided to put objective language in the requirement and use the Measures to show examples of more detailed lists of items.

Rationale for Requirement R1 Part 1.1

The SDT brought the security objective to the forefront in this requirement part by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the SDT made conforming changes to Applicable Systems to add SCI. The SDT considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories.

The SDT used the objective language "…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 and CIP-007, as defined by the Responsible Entity." The intent is to bound the scope to those changes that affect the system's CIP security posture. More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements.

The phrasing "alter the behavior of one or more cyber security controls" is intended to help clarify the scope. For example, the intent is that a user changing their password is not in scope; that is a change that may be required on some periodicity by a cyber security control such as a domain password policy but is not a change that alters the behavior *of the control itself*. What would be in scope is a change to that domain password policy.

The "excluding procedural and physical controls" (as well as the "*cyber security* controls" phrase) is intended to exclude from CIP-010 R1's scope changes to controls from CIP-005 and CIP-007 that are not technical controls. An example would be an entity may have signage or port-blockers as a procedural/physical control for meeting CIP-007 R1.2 concerning physical ports. Installing/removing port blockers or changes to the signage is not intended to be subject to CIP-010 R1. A change to the affinity rules for a hypervisor, if the entity uses that in an SCI scenario to meet CIP-007 R1.3, would meet the intent, as well as changes to EAP firewall rules/policy that the entity uses as the control to meet CIP-005 R1. The configuration of anti-malware controls the entity uses, such as update mechanisms or alerting mechanisms that change *how* the control functions in meeting CIP-007 R3 would be included but not the regular signature updates the control uses; those are not changes to the control's configuration that alter the way the control behaves.

Along these lines, rather than including a prescriptive list of change categories or types within the requirement, the SDT did analyze the requirements in CIP-005 and CIP-007 and included examples of cyber security controls that may serve those requirements in the Measures column to help clarify the intent. These are examples and are not a mandatory prescriptive list of the types of changes that would be included and for which evidence of authorization through change records could be provided.

It is important to note the SDT did not include prescriptive timeframes for this requirement. The rationale for this is to account for emergency changes, those that need to occur for reliability of the system when it may not be possible to put in a request and gain authorization beforehand. The SDT intent is for these system reliability related emergency changes to not become a violation of this standard, which it would if it had "prior to" type phrases within it, or required prescriptive definition of what constitutes emergency changes, etc. However, emergency changes will still need to be authorized, after the fact, to meet the requirement.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization.

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of permitting "CIP Exceptional Circumstances" in Pat 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with conforming changes to remove the 'baseline configuration' terminology and instead referring to operating systems, firmware, software, or software patches changes as the trigger for the Requirement Part.

The SDT acknowledges virtualization vendors may provide a "golden image" to clone multiple other Virtual Cyber Assets as described in the "Parent/Child Images" section above. The SDT intent is for entities that use the golden image technology to account for the software source and integrity of the golden image which covers any unmodified clones derived from it.

Rationale for Requirement R1 Part 1.4

Requirement Part 1.4 is a simplified version of the same part 1.4 in the previous version. The SDT made conforming changes to align the scope of this part with 1.1 with the phrasing "As a part of the changes authorized per Part 1.1…".

It is important to note the SDT intent and rationale behind the wording "As a part of the change". The rationale for that phrase is the entity, before closing out that change, will verify that the change has not adversely affected the cyber security controls. If the entity, as part of the post change verification, finds that it did, the entity must remediate that issue. The intent is this change cannot be completed until it is verified that the cyber security controls are not adversely affected.

What was 1.4.1 in the previous version required the entity to determine, prior to the change, the CIP-005 and CIP-007 controls that might be affected. With the automated remediation technology at instantiation, this is no longer possible and the SDT considered it was not the security objective. The security objective, the required behavior, is that entities ensure that changes don't adversely affect the cyber security controls by verifying them after making the change. That is now the clearly stated focus of 1.4. It is not the SDT's intent that the entity must test *every* cyber security control for *every* change, which is the rationale for the wording "of the altered cyber security controls". If an entity is installing a patch to an application on a BCS, it's not the intent that the entity verify that the domain password policy wasn't changed, however, the entity should verify the patch did not open or enable any unnecessary ports for example. The requirement part 1.4.3 from the previous version to document the results of the verification has been deleted and the SDT rationale is that is essentially a requirement to provide evidence for the actions taken to comply with the requirement part. Therefore 1.4 is now a simplified security objective to be met.

The rationale for the phrasing of "adversely affected" is simply to recognize that the desired effect of a change may be to impact a cyber security control – for example, an entity may wish to change a password policy such that it requires stronger passwords than the CIP standard requires. That would not be an "adverse" change.

Requirement R2

General Considerations for Requirement R2

The SDT has reworked R2 for monitoring for unauthorized changes to work better with the additional scope of R1's change management. The SDT's rationale is that all changes that should be included and authorized in a change management program may not have an automated solution for monitoring for unauthorized change and the SDT's intent is for this requirement's scope to be items that can be monitored by technical controls. Therefore, the SDT tied R2 loosely to R1's scope but with a required list of seven cyber security-related categories to monitor. The SDT's intent is to keep the scope of R2 to those things for which there are automated solutions that can monitor these areas and alert entities to changes.

The SDT has added the term "unauthorized" into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, the SDT is allowing for a capability that may filter out authorized changes such that the entity can have methods to monitor for unauthorized changes only. The SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.

The SDT has used the phrasing "that include at least one cyber security control for each of the following" in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing's intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required.

For the seven required control categories, the SDT notes it intent as follows:

2.1.1 – The intent is to monitor for changes to the system's configuration affecting ports or services that are enabled such that they provide accessibility via routable protocols on a network interface.

2.1.2 – The SDT notes that the intent of this item is conditional – evidence for this is only required "on SCI." If there is no SCI, then no control is required. If SCI is in scope, then some control to monitor for unauthorized changes to CPU/memory sharing of VCAs (affinity rules, etc.) is required.

2.1.3 - The intent of this is the traditional monitoring of changes to executable code of the various listed types. As noted in the Measures column, the SDT intends to handle the parent/child image issues by monitoring the parent image from which temporary child images are derived. See the "Parent/Child Images" section earlier in this document for examples.

2.1.4 – The intent is to monitor for unauthorized changes to the configuration of malicious code protection methods, for example whether they have been disabled, or alerting turned off, etc. Note this is not the detection or alerting or remediation of malicious code that is covered in CIP-007; this is monitoring the configuration of your method to ensure its configured behavior has not been changed in an unauthorized manner.

2.1.5 – Similar to 2.1.4, this is not monitoring the security event log and alerting as covered in CIP-007; this is monitoring the configuration of your security event logging and alerting for unauthorized changes that would change its expected behavior (disabling it, changing what is logged, changing where alerts go, etc.)

2.1.6 – The intent of "configuration of authentication methods" is to monitor for configuration changes that affect how a system authenticates its users/processes. Examples would include password policies (not individual user passwords), configuration of multi-factor authentication, changes to Pluggable Authentication Modules (PAM) on Linux systems, etc.

2.1.7 – Along with 2.1.6 concerning how a system is configured to authenticate users, this requires a control to monitor for unauthorized changes to enabled or disabled status of accounts. For example, if a "Guest" account or a default "admin" account have been disabled on a system, monitoring for the unauthorized re-enabling of those accounts.

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The previous language of "Prior to adding a new applicable Cyber Asset to a production environment" for the timing of performing a vulnerability assessment has an interesting "chicken or egg" problem when it comes to VCAs. This phrasing for the timing has worked well for hardware "programmable electronic devices" arriving on a loading dock or spares coming in from a warehouse that should be assessed before being physically placed "in production". However, VCA's aren't shipped, they are created in the production environment from a hardware perspective. A VCA image may be created on the hypervisor, an OS installed, the appropriate applications installed, etc., but the VCA is not yet connected to its production network and instantiated in a way that it has connectivity or is performing its function. However, it is from a hardware standpoint in the "production environment" so you can't do an assessment "prior to" that as this is where it's created.

To solve this issue, the SDT replaced this timing phrasing with the language "Prior to becoming a new Applicable System…". The SDT's rationale is the requirement part requires the vulnerability assessment at a point prior to the VCA being instantiated, with the "production" connectivity it requires, to perform its function either as a part of a BES Cyber System or EACMS or PCA. As it begins to perform those functions (i.e., for an EACMS to begin controlling or monitoring electronic access), it becomes an "Applicable System" at that point – prior to that point in time the vulnerability assessment of that VCA should have taken place. The remediation VLAN technologies may perform this automatically at every instantiation. The SDT made this change so that the requirement part did not imply that VCAs had to be created elsewhere, in some other separate hardware environment, assessed, and then somehow imported.

Conforming changes have been made to remove the baseline configuration dependency. The exceptions are "Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or CIP Exceptional Circumstances".

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4 and applies throughout Attachment 1.

The SDT also added an option to the software vulnerability mitigation portions of Attachment 1, Parts 1.3 and 2.1 for “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution”. This option has been added to point to “VM player” type technologies that will run a virtual image as a VCA in an immutable manner, not allowing changes to the image in order to mitigate exploitation of any software vulnerabilities in the image. The SDT’s intent is this is a virtualization-based equivalent to a live operating system booted from read-only media. Virtualization can also offer such options as “snapshots” where any changes to the image are written to a temporary file and discarded when the VCA is shut down, thus restoring it to a pristine state at next instantiation.

The SDT also made several other conforming changes to Attachment 1 for TCAs to ensure continuity in language between the measures and similar sections in CIP-003 Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section 6. Background has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP 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 standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. 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 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 UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems 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 (EACMS)** – 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 (PACS)** – 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 (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf
[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible.

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-

010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical

Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains an as-is “cut and paste” of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-010-3 to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity’s use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible

Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity’s personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity’s plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.