NATF Document for Implementation and Use of Transient Cyber Assets (TCAs) – NERC Reliability Standard CIP-010-2 Requirement R4, Attachment 1, Sections 1 and 2

This document was submitted to NERC for consideration as compliance "Implementation Guidance" on 9/26/17. NERC will review and post a decision on its website.

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve security. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

NERC Standards Implementation Guidance

Title of Implementation Guidance: Implementation and Use of Transient Cyber Assets (TCAs)
Standard Number: CIP-010-2
Standard Title: Cyber Security — Configuration Change Management and Vulnerability Assessments
Requirement(s): Requirement R4, Attachment 1, Sections 1 and 2
Date Submitted: xxx
Date Endorsed by ERO: xxx

This document is designed to assist Registered Entities (RE) with the implementation of this standard. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this guidance is not a substitute for compliance with requirements in NERC's Reliability Standards.

Purpose of Implementation Guidance

The purpose of this Implementation Guidance is to provide ERO-endorsed examples or approaches to illustrate how REs could comply with a standard that has been vetted by industry and supported by the ERO enterprise. The examples provided in this Implementation Guidance are neither exclusive nor all inclusive. Use of these Electric Reliability Organization (ERO) enterprise-endorsed examples provides a level of assurance that the ERO Compliance Monitoring and Enforcement Program (CMEP) staff will grant deference to the examples addressed in this document when conducting compliance monitoring activities. REs can rely upon the examples and be reasonably assured that they are meeting compliance requirements – keeping in mind that compliance determinations ultimately depend on facts, circumstances, and system configurations.

Background on Requirement and Associated Examples

Security requirements for Transient Cyber Assets (TCA), as defined in CIP-010-2 R4, became effective 4/1/2017. This document assesses various TCA approaches and strategies developed by North American Transmission Forum (NATF) members. This demonstrates a range of acceptable approaches that meet the objective for compliance with the Standard. Additionally, this document includes informal definitions of terminology associated with the Standard that were not defined in CIP-010-2 R4. These informal definitions provide a common framework for understanding the concepts behind the approaches described in this document.

Definitions:

On-demand compliance model – use of a checklist to validate security status of an individual Transient Cyber Asset just prior to connecting it to a BES Cyber System, a network within an ESP, or a PCA.

Ongoing compliance model – use of a preauthorized inventory of secure Transient Cyber Assets that are continuously compliant and may be used at any point in time for approved TCA functions

Transient Cyber Asset (TCA) – refer to NERC Glossary of Terms

Implementation Approach

Entities have great flexibility in determining what types of devices can be authorized for use as TCAs, where they can be deployed, and how these devices are used and managed. The NATF has documented and evaluated multiple approaches as a means of demonstrating a range of acceptable options for technical implementation that meet compliance. For this analysis, various NATF members contributed information about TCA strategies developed by their organizations.

Based on the Standard, the tables below show a wide range of implementation strategies. While there are other approaches, including combination approaches, these tables provide a summary of common options that could be used, based on the two compliance management models (On-demand and Ongoing, respectively). Several assumptions made in developing this guidance:

- Use of the On-demand compliance model requires that an entity document each TCA usage event to demonstrate compliance. (Note: Because of this additional compliance process and documentation, exclusively on-demand strategies were not explored in detail for this document.)
- Use of the Ongoing compliance model does not require generation of compliance documentation for each TCA use.
- TCAs may be "dedicated," meaning they are authorized only to perform TCA functions, and may not be used for other business or non-business functions.
- TCAs may be "non-dedicated," meaning they are authorized for TCA use in addition to other business uses.
- TCAs may be assigned to specific people or locations.

TCA Strategy Summary: On-Demand Compliance Model

TCA Assignment Type	Dedicated to the TCA Function?	Comments	Security Notes
Location-based TCA: fixed location	Yes - Dedicated TCA	Device is a dedicated TCA assigned permanently to one location, authorized for use by one or more approved individuals following a documented on-demand compliance check.	The approved location should supply connectivity to a corporate/secure network, as the TCA requires access for software and anti-virus verification as part of the on-demand check required prior to TCA use.
Location-based TCA: multiple locations (roaming)	Yes - Dedicated TCA	Device, or pool of devices, dedicated for TCA use at multiple authorized locations, by one or more approved individuals following a documented on-demand compliance check.	Connectivity to a corporate/secure network is needed for software and anti-virus verification as part of the on-demand check required prior to TCA use.
Personnel-based TCA: assigned to one person (TCA Owner)	Yes - Dedicated TCA	Device is a dedicated TCA assigned to a person who is authorized to use that TCA at one or more approved locations following a documented on-demand compliance check.	Connectivity to a corporate/secure network is needed for software and anti-virus verification as part of the on-demand check required prior to TCA use.
Personnel-based TCA: assigned to multiple people	Yes - Dedicated TCA	Device is a dedicated TCA assigned to a pool of users authorized to use that TCA at one or more approved locations following a documented on-demand compliance check.	Connectivity to a corporate/secure network is needed for software and anti-virus verification as part of the on-demand check required prior to TCA use.
Personnel-based TCA: assigned to one person (TCA Owner)	No - Non-dedicated	A single device, assigned to an Owner; authorized for multiple uses (TCA use, as well as other business activities) at one or more approved locations. Approved for TCA use only following a documented on-demand compliance check.	TCA Owner is responsible for securing the device, physically and electronically. The device is configured to support two operating modes (Business User Mode, TCA User Mode). At least one of the approved locations should supply connectivity to the corporate network, as the TCA requires access for software and anti-virus verification as part of the on-demand check required prior to TCA use.
Other - vendor supplied and supported device	Yes - Dedicated TCA	Vendor supplied/Vendor supported device, or pool of devices, dedicated for TCA use at multiple authorized locations, by one or more approved individuals. Approved for TCA use only following a documented on-demand compliance check.	Vendor is responsible for securing the TCA electronically, and with RE oversight, must provide support for on-demand check required prior to TCA use.

TCA Strategy Summary: Ongoing Compliance Model

Assignment Type	Dedicated to the TCA Function?	Comments	Security Notes
Location-based TCA: fixed location	Yes - Dedicated TCA	Device is a dedicated TCA assigned permanently to one location, authorized for use by one or more approved individuals	Connectivity to a corporate/secure network is needed for periodic access to software and anti-virus updates.
Location-based TCA: multiple locations (roaming)	Yes - Dedicated TCA	Device, or pool of devices, dedicated for TCA use at multiple authorized locations, by one or more approved individuals.	Connectivity to a corporate/secure network is needed for periodic access to software and anti-virus updates.
Personnel-based TCA: assigned to one person (TCA Owner)	Yes - Dedicated TCA	Device is a dedicated TCA assigned to a person who is authorized to use that TCA at one or more approved locations	TCA Owner is responsible for securing the device physically. Connectivity to a corporate/secure network is needed for periodic access to software and anti-virus updates.
Personnel-based TCA: assigned to multiple people	Yes - Dedicated TCA	Device is a dedicated TCA assigned to a pool of users authorized to use that TCA at one or more approved locations	Connectivity to a corporate/secure network is needed for periodic access to software and anti-virus updates.
Personnel-based TCA: assigned to one person ("TCA Owner")	No - Non-dedicated	A single device, assigned to an Owner; authorized for multiple uses (TCA use, as well as other business activities) at one or more approved locations	TCA Owner is responsible for securing the device physically. The device is configured to support two operating modes (Business User Mode, TCA User Mode). At least one of the approved locations should supply connectivity to the corporate network, as the TCA requires periodic access for software and anti-virus updates.
Other - vendor supplied and supported device (Vendor-Assisted)	Yes - Dedicated TCA	Vendor supplied/Vendor supported device, or pool of devices, dedicated for TCA use at multiple authorized locations, by one or more approved individuals.	Vendor is responsible for securing the TCA electronically, and with RE oversight, must provide support for ongoing compliance.

Assessment

The NATF assessed this range of implementation options for both compliance models and suggests that:

- A TCA program should be governed by a documented policy, program, or procedure that establishes the basis for TCA security, compliance and user expectations. This governing document should provide the RE's requirements for protecting, securing, validating, and using TCAs, such as:
  - Approved TCA locations

- Approved TCA functions (testing, maintenance, etc…)
- Prohibited TCA activity: e.g. no internet, email, or non-secured networks during use as a TCA. No dual or multi homing while a TCA is in use.
- General: TCAs subject to the ongoing compliance model, and deemed to be in a secured and compliant state, may be designated for use on all CIP system impact levels (High, Medium and Low), as well as non-CIP cyber assets.
- Note: The on-demand compliance model, if used solely, should include a comprehensive security check documented just prior to connecting it to a BES Cyber System, a network within an ESP, or a PCA.

Implementation approaches for the ongoing compliance model and/or combination (of ongoing and on-demand) model are described in detail in Appendix 1 of this document. The approaches are documented herein as responses to the individual parts of Attachment 1, Sections 1 and 2. Note: these responses appear as italicized text in Appendix 1.

Note that Attachment 1, Section 3, Removable Media, is not in the scope of this document.

In Appendix 2 of this document, an alternative approach is provided. This approach involves the use of Protected Cyber Assets (PCA) rather than TCA.

Appendix 1: TCA Implementation Approaches – the Ongoing Compliance Model

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.

Response:

(1) Managing TCAs in an ongoing manner

As defined in this document, managing TCAs in an ongoing manner involves "use of a preauthorized inventory of secure TCAs that are continuously compliant and may be used at any point in time for approved TCA functions." It is important to note that a TCA is only a TCA while it is in active use as a TCA: "directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA." Authorized devices may be used for other approved business purpose while not being actively used for TCA functions. Last, "dedicated" devices are used exclusively for TCA functions. "Non-dedicated" devices either operate in multiple modes or have controls in place to allow TCA functions to be performed.

Ongoing compliance requires that an approved device be in a secure state, ready for use at any time for TCA functions. Security controls must be implemented that mitigate both malicious code and software vulnerabilities, e.g. leveraging enterprise security patch management and anti-virus endpoint programs. TCAs should be connected to the corporate (or secure) network regularly to update anti-virus signatures and receive software updates. The RE must establish a procedure that defines this process.

Technical, procedural, and administrative controls allow these TCAs, managed in an ongoing manner, to be used on all CIP system impact levels (High, Medium and Low), as well as non-CIP cyber assets.

Location-based TCAs: Ongoing Compliance Model

Network connectivity at remote substations provides ability to support this approach:

- ***Fixed Location TCAs*** *– one or more devices dedicated to the TCA function are permanently located at a facility where they can regularly connect to the corporate (or secure) network for software and anti-virus updates. These types of TCAs are subject to an ongoing compliance model, and are:*
  - *configured exclusively for defined TCA functions (e.g. testing, maintenance, recovery of local devices)*
  - *located permanently at authorized, secured locations,*
  - *approved for use only by approved personnel,*
  - *designated for use on all CIP system impact levels (High, Medium and Low), as well as non-CIP cyber assets.*
- ***Roaming TCAs*** *- a pool of devices that are dedicated to the TCA function and are regularly connected to the corporate (or secure) network for software and anti-virus updates and are:*

- *configured exclusively for defined TCA functions (e.g. testing, maintenance, recovery of local devices),*
- *located at authorized, central locations, for use only by approved personnel,*
- *approved for "check-out" and transport. Authorized personnel are permitted to check-out and transport these devices to other approved locations for TCA functions, to be used interchangeably.*
- *returned or connected to the RE corporate network following checkout as specified in the RE TCA procedure.*
- *suitable for use on all CIP system impact levels (High, Medium and Low), as well as non-CIP cyber assets.*

Personnel-based TCAs: Ongoing Compliance Model

This approach can leverage the use of existing enterprise programs for patch management and anti-virus signature updates. This approach can include:

- ***Personnel-based Dedicated TCAs** – approved personnel are assigned TCA's (e.g. a second laptop). These "dedicated" devices are regularly connected to the corporate (or secure) network for software and anti-virus updates, comprising an ongoing compliance model, and are:*
  - *configured exclusively for defined TCA functions (e.g. testing, maintenance, recovery of local devices),*
  - *approved for use only by the device owner ("TCA Owner")/assignee*
  - *may be transported and used as a TCA by the assignee at any authorized location*
  - *approved for use on all CIP system impact levels (High, Medium and Low), as well as non-CIP cyber assets.*
- ***Dedicated Vendor-Assisted TCAs** – another approach is to use a third-party device as a TCA. The third party provides and maintains the hardware platform and facilitates patching and malicious code mitigation in an on-going manner, with oversight from the RE.*
- ***Non-Dedicated, "Dual-mode" option** - the corporate-managed laptop, assigned to an individual, has a logical configuration that provides two separate modes of operation (a "TCA Mode" and a "Corporate Mode"). In this approach, the user has only one laptop. These devices are:*
  - *configured for defined TCA functions (e.g. testing, maintenance, recovery of local devices) only in TCA mode*
  - *approved for use only by the device owner/assignee*
  - *may be transported and used as a TCA by the assignee at any authorized location*

(2) Managing TCAs in an on-demand manner

The "on-demand model" requires extensive additional compliance documentation. NATF members did not provide specific accounts of using an exclusively on-demand TCA strategy. Thus, that approach was not explored as part of this guidance.

(3) Managing TCAs in a manner combining ongoing and on-demand compliance models

This approach leverages use of enterprise programs for patch management and anti-virus updates, and provides the advantage that the devices are already assigned to designated employees and/or contractors. While these devices are running in a "single mode of

operation," a combination of procedural and administrative controls are exerted to meet compliance.

Individually-assigned TCAs: Combined Ongoing/On-demand Compliance Model

- ***Non-Dedicated TCAs*** *– non-dedicated devices are exposed to more risk as multi-purposed machines. These corporate devices should require frequent updates for patching and anti-virus. They should be part of a program that includes these procedural and administrative controls in support of the ongoing compliance model:*
    - *Enhanced awareness and training focused on appropriate use and restrictions*
    - *Physical Access requirements to limit risk*
    - *Encryption used to protect data at rest*
    - *System hardening (e.g. removal of unnecessary software, verification that only certified software versions are installed)*
    - *Limit any administrative privileges granted to users*
    - *Connection to the internet is prohibited during active TCA use*
    - *Monthly security patch assessment of all third-party software*
    - *Security Patch implementation, as established in the REs TCA procedures*

- *Since these devices are used for multiple purposes, additional procedural checks should be executed prior to connection of a TCA to a BES Cyber Asset, a network within an ESP, or a PCA. The on-demand TCA check should verify that anti-virus updates are current and software versions are valid.*

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;
Response:
Authorization for use of specific TCAs, or groups of TCAs, should be identified, approved, and tracked by individual TCA and individual TCA user/groups of users. Once documented at the individual TCA and TCA user level, each may be grouped for provisioning purposes.

TCA usage authorization should require at least one level of approval (e.g. from the TCA Owner). Note: TCA user access is not subject to CIP-004 program level requirements, e.g. Personal Risk Assessment (PRA) or Training). However, unescorted physical and electronic access to the Cyber Assets that TCAs are connected to does require CIP-004 authorization.

1.2.2. Locations, either individually or by group; and

Response:
Entities should identify and document which locations are authorized for TCA use. Those locations should be tracked and retained as part of the program management. Grouping approved locations may have value in provisioning.

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

TCAs should be authorized for specific approved functions and documented in the RE TCA procedure. Approved functions should include but not be limited to software/firmware updates, uploading new or modified configurations, downloading configurations, changing passwords, and other functions necessary for the support, maintenance, replacement, recovery or documentation of a BCA or a PCA at any approved location.

Business functions should not include use of the Internet, email, or non-secure/unauthorized network access while the device is in active use as a TCA (i.e. while the TCA is actively connected to a BES Cyber Asset, a network within an ESP, or a PCA). Use of the Internet, Wi-Fi, or email should be prohibited, and if possible, technically impeded during active TCA use.

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.

Response:

- *Mitigation of software vulnerabilities posed by unpatched software can be addressed on multiple fronts: Operating systems and corporate-maintained software (e.g. word processing applications), can be subject to automated enterprise-level patch management*
- *TCA application software used to perform approved business functions and third-party software may be managed with a manual assessment and patching process*

As stated previously, TCAs employing the ongoing compliance model are subject to enterprise patch management, including automated OS patching. TCAs should be regularly connected to the corporate (or secure) network for patch management.

TCA application and other third-party software vulnerabilities can be mitigated via manual security patching processes. Any TCA approved third-party software (such as testing application software used to perform business functions) should be evaluated for applicable security-related patches prior to deployment onto the TCA. Additionally, any new applications/software approved for use on a TCA should be certified, then integrated into a structured security patch management process for ongoing support.

In the case of vendor-assisted TCAs, any application software patch deemed applicable is thoroughly tested by the vendor. Once approved for production, the vendor should schedule a staged release/field test to a sub-set of devices. Following successful field testing, the vendor can push the approved update to the rest of the general user population.

Another approach to mitigating software vulnerabilities is a form of system hardening, known as application whitelisting (AWL). AWL permits only authorized applications and processes to run. AWL should involve a rigorous evaluation of all software proposed as needed to operate the TCA. Approved software should be certified and patched prior to

deployment on the TCA. The AWL must be maintained and software should be integrated into a patch management process that, at a minimum, assesses and implements security patches on a quarterly basis.

Last, while in use as a TCA, access to the internet, connectivity to untrusted networks, and wireless/cellular communications should be prohibited.

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.

Response:
As stated previously, TCAs employing the ongoing compliance model are subject to an enterprise-level endpoint anti-virus management program. TCAs should be regularly connected to the corporate network for anti-virus signature updates.

System hardening may also be employed, including removal of all non-essential software, application whitelisting, and where possible, application blacklisting.

In the case of vendor-assisted TCAs, one member documented a process where managed updates of signatures for the antivirus software are provided by the vendor on a regular basis, via a private LTE connection. There is no direct connection to the Internet possible through this method.

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.

Response:
Entities employed a variety of methods to prevent unauthorized use of TCAs:
Restricting physical access: Location-based TCAs

- *Dedicated TCAs located at Medium Impact substations are stored in a PC lock box within the associated PSP of the Medium Impact Substation.*
- *TCAs located within physically controlled Electric Transmission main offices or Electric Transmission field offices require authorized card key access to the controlled area doors. These TCAs are under the control of authorized users when removed from those locations.*

Restricting physical access: Employee-assigned TCAs

- *TCAs are kept in a physically secured area when not in use. They must be under the control of authorized users when removed from the main office.*
- *TCAs are assigned to employees who are authorized to use them as TCAs only at specified approved locations. Employees are required to protect and store these devices appropriately, thus restricting physical access to the device.*
- *Access to the "TCA Mode" is restricted to users who have the proper Active Directory username and password, as well as an RSA Token (issued to authorized users) and PIN providing a second authentication factor.*

Full-disk encryption with authentication: Employee-assigned Vendor-assisted TCAs

- *Third-party TCAs could require a boot-up login to allow access to the encrypted hard drives. After booting up, an additional login should be required for actual usage. The individual authorized engineer to whom the TCA is assigned is responsible for the physical security per standard security procedures. (The security procedures include but are not limited to secure storage of the physical device, preventing unauthorized use, etc.)*

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.

Response:
Vendor or third-party TCAs may be used, but only under specified conditions and with rigorous oversight. For ad hoc, unplanned or emergency use of a vendor TCA, the entity should mitigate risk of vulnerabilities posed by unpatched software from the vendor device. To accomplish this, the entity must, at a minimum, thoroughly review and approve the third-party patching process. Additionally, at least one these other methods should be applied prior to authorizing use of a third-party device for TCA functions:

- *removal of all non-essential software, AWL, and where possible, application blacklisting.*
- *an inventory of the installed software on the vendor TCA must be provided by the vendor. That list should be evaluated for any existing/known security patches and vulnerabilities. Security patches should be assessed for applicability and applied as indicated. The inventory should be maintained on an ongoing basis by the vendor, with quarterly updates to the entity.*
- *The vendor should supply documentation regarding any open mitigation plans or other methods they use to mitigate 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.

Response:

Vendor or third-party TCAs may be used, but only under specified conditions and with rigorous oversight. For ad hoc, unplanned or emergency use of a vendor TCA, the entity should mitigate the risk of malicious code. To accomplish this, the entity must, at a minimum, thoroughly review and approve the third-party anti-virus process. Additionally, at least one these other methods should be applied prior to authorizing use of a third-party device for TCA functions:

- *confirm that antivirus software is installed on the device(s), with a policy for updating signatures on a regular basis (weekly, monthly or quarterly)*
- *If AWL is employed, confirm the product that was used and review its configuration*

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.

Response:

The entity should require that all electronic access points on the vendor device other than the physical connection used while completing the work order are disabled. This includes, but isn't limited to, disabling wireless radio and Bluetooth while the vendor device is connected to BCAs. The Standard Work Practices also require that all applications deemed unnecessary for completing the work order are closed.

APPENDIX 2: PCAS – AN ALTERNATIVE APPROACH TO THE USE OF TCAS

Scenario: Use of Protected Cyber Assets (PCA) as an alternative to use of TCAs.

Use of TCAs poses some level of security risk to BCS, even with defined security controls in place. One alternative is the elimination of TCAs, and their replacement with Cyber Assets that reside permanently within the ESP. These devices, classified as PCAs, are fully protected by both an ESP and a PSP. However, they are subject to many more NERC CIP requirements, require extensive compliance documentation and attention, and pose compliance risks that TCAs do not. The following section describes how an entity may implement such a change.

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.

Response:
Use of dedicated PCs for configuration of field devices. The PCs are installed at CIP medium sites, remain connected inside the ESP network, and will be classified as PCAs (instead of TCAs).

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;

Response:
Not applicable.
Note that entities can elect to use existing CIP-004 Access Management programs to protect and authorize access to PCAs, but this is not required by the Standards.

1.2.2. Locations, either individually or by group; and

Response:
Not applicable.

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

Response:
Not applicable.
While not required, PCAs would be authorized for any approved functions necessary for the support, maintenance, replacement, or documentation of a BES Cyber Asset or a PCA at any approved location.

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;
- Other method(s) to mitigate software vulnerabilities.

Response:
Not applicable.
PCAs are afforded similar protections against many vulnerabilities, including monthly patching and configuration management (e.g. hardening/removal of unnecessary ports and services).

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.

Response:
Not applicable.
Note that PCAs are subject to CIP-007 R3.2. Corporate antivirus endpoint software could be used to protect these devices if available at field locations.

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.

Response:
Not applicable.
PCAs are afforded protections of the ESP and PSP. Unauthorized use will be mitigated by restriction of physical access and multi-factor authentication (if applicable). Only users who have unescorted physical access to the control house will have physical access to the device. RSA tokens will be used to provide multi-factor authentication for cyber access to the device.

2. SECTION 2. TRANSIENT CYBER ASSET(S) MANAGED BY A PARTY OTHER THAN THE RESPONSIBLE ENTITY.

Response:
Use of Vendor-managed TCAs is not applicable to this example.

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.

Response:
Use of Vendor-managed TCAs is not applicable to this example.

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.

Response:
Use of Vendor-managed TCAs is not applicable to this example.

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.
Response:
Use of Vendor-managed TCAs is not applicable to this example.