North American Transmission FORUM

Community Confidentiality Candor Commitment

This document was submitted to NERC for consideration as "Implementation Guidance. Visit NERC's compliance guidance website for more information.

NATF Transient Cyber Asset Guidance

Disclaimer
This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. 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.

Version 2.0
Document ID: 1063
Approval Date: 12/04/2019

Versioning

Version History

Date	Version	Notes
10/16/2017	1.1	Original issue
12/04/2019	2.0	Revised implementation approach examples

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

1. Introduction

This document is designed to assist Registered Entities with the implementation of "NERC Reliability Standard CIP-010-2 Requirement R4, Attachment 1, Sections 1 and 2. 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.[1]

2. Background on Requirement and Associated Examples

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

3. Definitions

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

Models

Prohibited Use Model – Prohibition of the use of TCAs in BCS environments.

On-demand Use Model – Use of tools, such as, but not limited to, a checklist, to validate security status of an individual Transient Cyber Asset prior to connecting it to a BCS, a network within an ESP, or a PCA.

Ongoing Use Model – Use of a preauthorized inventory of secure Transient Cyber Assets that are maintained in a manner to assure continuous compliance and may be accessed and used by authorized personnel at any point in time for approved TCA functions.

[1] As stated in the November 5, 2015, Compliance Guidance Policy: "Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [footnote omitted] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard. The ERO Enterprise's endorsement of an example means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." *Available at:* http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

4. Scope

CIP-010-2 Requirement R4, Attachment 1 Sections 1 and 2, Transient Cyber Assets

High and Medium impact BES Cyber Systems (BCS) and associated Protected Cyber Assets (PCAs).

Note regarding references to "Low impact": Mandatory requirements for Low impact TCAs differ from the mandatory obligations of CIP-010-2 Requirement R4 to be commensurate with risk, and are therefore out of scope of this implementation guidance. This does not preclude Registered Entities from leveraging the concepts here in to go above and beyond those obligations by developing and implementing an enterprise TCA Program that collectively includes all impact-rated BCS.

Exclusions

CIP-010-2 Requirement R4, Attachment 1 Section 3, Removable Media

5. 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 evaluated and documented several approaches that meet the requirements of the standard.

5.1 Prohibited TCA Use

To minimize the security, reliability, and compliance risk associated with the use of TCAs, Registered Entities could consider strictly prohibiting the use of TCAs at an enterprise policy level to prevent connectivity to high and/or medium impact BCS.

Use of architectures and solutions to prohibit TCA use often requires additional technology logically located within the ESP that must be classified and protected as a PCA. The ability to ban the use of TCAs is highly dependent on the Registered Entities' technological capabilities and operational needs, as well as the physical mechanisms and detective controls available to assure no TCAs are used. For Registered Entities that rely on logical or remote connectivity mechanisms for access to or management of BCAs and/or PCAs, this may be a viable alternative to managing separate hardware to physically connect to BCSs on a temporary basis.

While this approach has the potential to relieve most of administrative burdens related to TCA management, there are tradeoffs. For example, some Registered Entities prefer to use local physical connections for construction, maintenance, or support activities because these connections allow employees to use visual techniques that improve safety and minimize the likelihood of misoperations or human performance errors that can occur when connecting remotely.

If considering this option, Registered Entities should recognize that this approach does not relieve the Registered Entity from compliance obligations for access management and authorization, Interactive Remote Access (IRA), External Routable Connectivity (ERC), nor interactive user access requirements and controls prescribed by CIP-002 through CIP-011 of the current enforceable Standards. Additionally, dated evidence including, but not limited to, a statement, policy, or other document that states TCAs are not used is required to demonstrate compliance.

As examples, the following configurations could be implemented individually or in any combination to achieve a TCA-free solution:

5.1.1 If conducive to the environment and infrastructure, a Registered Entity could permanently deploy routable Cyber Assets capable of and purposed for support, troubleshooting, and/or maintenance of a BCS within the ESP and protect them as PCAs. This provides controlled remote or locally routable management functions through a controlled and compliant PCA.

5.1.2 For serial connections to BCAs, a Registered Entity could implement technology like, but not limited to, serial communication processors (concentrators) containing a routable interface within the ESP. The communication processors are connected to the serial interfaces of BCAs and provide indirect logical or remote management functions through a controlled and compliant routable interface within the ESP.

5.1.3 To support adherence to a program that prohibits TCAs, the Registered Entity could:

- take measures to physically remove any I/O interface hardware/ports that are not in use,
- use physical controls to deter or prevent connectivity to unused I/O interface hardware/ports (i.e., port blockers, tamper tape etc.)
- if technically possible, configure monitoring and alerting of up/down status of used and/or unused I/O interface hardware/ports for detection of conditions where permanent connections are disrupted or where prohibited connections are made.

When using a prohibited TCA policy, local physical connectivity to a BCA or PCA, even if detected, may constitute non-compliance to CIP-010-2 Requirement R4.

The tables below include wide range of TCA implementation strategies. While there are other approaches, including combination approaches, these tables provide a summary of common options, based on the two compliance management models (on-demand and ongoing). Several assumptions are made in developing this guidance:

- Use of the on-demand compliance model requires that an entity generate and retain evidence of the TCA's verified security posture prior to BCS connection to demonstrate compliance.
- Use of the ongoing compliance model requires demonstration of how TCA access and security posture are managed when the TCA is not in use within a BCS, and supporting compliance evidence of the implementation of continuous controls that meet the objective of CIP-010-2 Requirement R4.
- Authorized functions for equipment designated as a TCA should be documented, whether the Cyber Asset is dedicated to use on BCSs or acceptable to use in unregulated environments as well. TCAs may be assigned to specific individuals, teams, functions, or locations. Whether allocated to a specified individual or designated for shared use, evidence of authorized users is needed to demonstrate compliance.

5.1.4 TCA Strategy Summary: On-Demand Use Model – Potential Approaches

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 secured private network/controlled logical environment, 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 secured private network/controlled logical environment 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 secured private network/controlled logical environment 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 secured private network/controlled logical environment 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 secured private network/controlled logical environment, 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 Registered Entity oversight, must provide reasonable assurance and supporting evidence that operational practices support for on-demand check are required and implemented prior to TCA use.

5.1.5 TCA Strategy Summary: Ongoing Use Model – Potential Approaches

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 secured private network/controlled logical environment 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 secured private network/controlled logical environment 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 secured private network/controlled logical environment 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 secured private network/controlled logical environment 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 Registered Entity oversight, must provide support for ongoing compliance.

5.2 TCA Program Governance

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 Registered Entity’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 within a BCS)
- General: TCAs whose posture has undergone ongoing or on-demand security verification, and which have been determined to be in a secured and compliant state, may be designated for use on all CIP BCS impact levels (High, Medium, and Low[2]), as well as any associated PCA.

> The on-demand compliance model, if used solely, should include a comprehensive security check documented just prior to connecting the TCA to a BCS, a network within an ESP, or any associated PCA.

6. Assessment of Implementation Options

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. A Responsible Entity may choose any one or combination of approaches, may alternate between approaches (with appropriate documentation), or may develop its own approach. The approaches are documented herein as responses to the individual parts of Attachment 1, Sections 1 and 2. These responses appear as italicized text in Appendix 1.

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

[2] Mandatory requirements for Low impact TCAs differ from the mandatory obligations of CIP-010-2 Requirement R4 to be commensurate with risk, and are therefore out of scope of this implementation guide. This does not preclude Registered Entities from leveraging the concepts here in to go above and beyond those obligations by developing and implementing an enterprise TCA Program that collectively includes all impact-rated BCS.

Appendix 1: TCA Implementation Approaches – the Ongoing Compliance Model

Implementation approaches for the ongoing compliance model and/or combination (of ongoing and on-demand) model are described below. A Responsible Entity may choose any one or combination of approaches, may alternate between approaches (with appropriate documentation), or may develop its own approach. The approaches are documented herein as responses (in italicized text) to the individual parts of CIP-010-2 Attachment 1, Sections 1 and 2.

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 (BCA), 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. "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 to mitigate both malicious code and software vulnerabilities (e.g., leveraging enterprise security patch management and anti-virus endpoint programs). TCAs should be reconnected to the secure private network/controlled logical environment in a timely manner after use to update anti-virus signatures and receive software updates. The Registered Entity 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 BCS levels (High, Medium and Low), as well as any associated PCA.

To demonstrate compliance, Registered Entities should consider how evidence is generated and retained.

- *Registered Entities who have implemented third-party tools to support configuration change management baselines for CIP-010-2 R1 may have technologies that could be leveraged to monitor status when the device is not in use as a TCA and is connected to the secured private network/controlled logical environment to receive updates. This approach could be used to retain critical evidence that demonstrates when the device was patched and when malware prevention signatures/pattern files were installed etc.*
- *Registered Entities that utilize network health monitoring tools could consider monitoring the network ports where devices not in use as TCAs are to be connected. Systems like this*

can send network interface status information when connectivity changes and can help demonstrate compliance with the ongoing model when compared to access records.

- *Another form of evidence that could be retained to demonstrate authorized use might be security event logs that record login/logoff activity, as well as any events that malware prevention tools may have discovered and addressed. Registered Entities could consider leveraging security status monitoring practices and/or technologies already in use to comply with CIP-007-6 R4 to capture these records. These records help provide traceability to the list of authorized personnel.*

- *When determining where the device will reside to receive continuous updates, consider if physical placement inside a PSP is an option. While not required, the potential to leverage existing physical security controls implemented to support CIP-006-6 can help to further demonstrate that access to Cyber Assets authorized for TCA use is physically restricted without incurring additional cost or having to implement separate administrative processes/controls. Because PSP access is reviewed quarterly pursuant to CIP-004-6 R4, this approach offers additional benefits to demonstrate physical access is restricted and authorizations are current.*

- *Registered Entities who have a Security Information and Event Management (SIEM) might consider sending data from multiple sources for consumption and cross correlation. Depending on the sophistication of the Registered Entity's tool suite, logical access, physical access, network interface status, patch installation, malware prevention tool signature/pattern updates, configuration change information, and/or security status events could be collected in a centralized system from which evidence could be extracted upon request during audit to demonstrate ongoing compliance.*

- *If choosing to implement the ongoing compliance model, Registered Entities may consider purpose-built solutions. There are commercially available products comprised of an environmentally-controlled cabinet equipped with power, network interfaces, and secured drawers designed to house a laptop and docking station. Some products like this can be integrated with existing card key reader systems to restrict and log physical access; others might use other cyber or crypto key technologies. Solutions like this may help make evidence collection more intuitive and alleviate the burden to demonstrate compliance.*

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 are connected to the secured private network/controlled logical environment for software and anti-virus updates when not in use as a TCA. 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 any associated PCA.*

- ***Roaming TCAs*** *- a pool of devices that are dedicated to the TCA function and are reconnected to the secured private network/controlled logical environment for software and anti-virus updates while when not in transit or not use as a TCA 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 Registered Entity corporate network following checkout as specified in the Registered Entity 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 existing enterprise programs for patch management and anti-virus signature updates. This approach can include:

- ***Personnel-Based Dedicated TCAs*** *– approved personnel are assigned TCAs (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 Registered Entity. If choosing this implementation approach, consider acquiring the third party's process documentation and reviewing it for sufficiency to expectations. Another option to consider is a written contract with the third party (i.e., a Memo of Understanding (MOU) or Letter of Agreement (LOA)) that includes provisions for cyclical reviews of process documentation, Registered Entity involvement and approval for any off-cycle process changes/updates, and/or a clause that allows the Registered Entity to audit the third party's implementation to provide reasonable assurance controls are operating as designed. Terms of engagement like this can be beneficial to demonstrating compliance when undergoing audit.*
- ***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, and securely stored when not in use*

(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, experience with that approach is limited. For Registered Entities who want to consider this approach, the establishment and implementation of standardized practices could help assure consistent evidence is captured.

- *Job aids such as, but not limited to, a checklist of the checks to perform, supplemented with instruction on what system-generated evidence to collect when the verification is performed, might be one approach. Filling out a checklist alone may not suffice, since a checklist is merely an attestation. Supporting this with corresponding dated records that depict the actual configuration provides the extra rigor to substantiate the device's posture was aligned with the conclusions of the checklist. System-generated evidence could be in the form of command line outputs, configuration or registry exports, system or application logs, screenshots of settings, batch file or script outputs, or other mechanisms capable of capturing the point-in-time security posture.*
- *For Registered Entities using third party tools to baseline and/or monitor BCAs and associated Cyber Assets pursuant to CIP-010-2 R1 and/or R2, consider leveraging that technology to accomplish and record evidence of on-demand security verification. Implementing practices or technical controls that cause the system to routinely monitor for, detect, and interrogate devices approved for the on-demand method, or solutions that cause the on-demand TCA to "check-in" upon network connection could help automate this process, offer consistency and repeatability, and may have the capability to collect and retain evidence as a byproduct to demonstrate compliance during audit.*

(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 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 Registered Entity's TCA procedures*

Since these devices are used for multiple purposes, consider additional procedural checks to be executed prior to connection of a TCA to a BCA, a network within an ESP, or a PCA. At a minimum, the on-demand TCA check should verify that applicable security patches are applied, anti-virus updates are current, and software versions are valid. For Registered Entities using third party tools to baseline and/or monitor BCAs and associated Cyber Assets pursuant to CIP-010-2 R1 and/or R2, consider leveraging that technology to accomplish and record evidence of on-demand security verification. Implementing practices or technical controls that cause the system to routinely monitor for, detect, and interrogate devices approved for the on-demand method, or solutions that cause the on-demand TCA to "check-in" upon network connection could help automate this process, offer consistency and repeatability, and may have the capability to collect and retain evidence as a byproduct to demonstrate compliance during audit.

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., Personnel 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 Registered Entity 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 BCA, 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 employ 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

- *Vendor-assisted 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 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 are closed.

Appendix 2: PCAs – An Alternative Approach to the Use of TCAs

Scenario:
Use of Protected Cyber Assets (PCAs) 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, and require extensive compliance documentation and retention. 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 authorized 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.

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:

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.