
Compliance
FUNDAMENTALS
November 14, 9:00 a.m. to 12:00 p.m. Mountain

<Public>

WECC

Low Impact Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

November 14, 2024

Jennifer Salisbury, Auditor

and Tyler Whiting, Senior Auditor

Agenda

- Terms
- Cybersecurity Plans
- Methods
- Implementation Artifacts
- Recommendations

CIP Exceptional Circumstance (CEC)

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large-scale workforce availability.

Removable Media (RM)

Storage media that:

- Are not Cyber Assets
- Can transfer executable code
- Can be used to store, copy, move, or access data
- Are directly connected for 30 consecutive calendar days or less to a
  - BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems
  - Protected Cyber Asset associated with high or medium impact BES Cyber Systems

Examples: Floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory

Transient Cyber Asset (TCA)

Cyber Asset that is:

- Capable of transmitting or transferring executable code;
- Not included in a BES Cyber System;
- Not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems; and
- Directly connected for 30 consecutive calendar days or less to a:
  - BES Cyber Asset;
  - Network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems; or
  - PCA associated with high or medium impact BES Cyber Systems

Examples: Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

slido

Do you allow the use of TCA or RM to connect to your low impact BES Cyber Systems?

ⓘ Start presenting to display the poll results on this slide.

TCA & RM Cybersecurity Plan(s)

Have one or more plans for malicious code risk mitigation for the use of TCA or RM

The TCA plan(s) must **document the methods** used to mitigate the introduction of malicious code for:

- TCA managed in ongoing or on-demand manner
- TCA managed by a party other than the Responsible Entity, and if any additional mitigation actions are needed, before connecting the TCA

The RM plan(s) must document the methods used to detect malicious code and mitigate the threat of malicious code before connecting RM

Management of TCA

- TCA managed in an ongoing manner
  - Controls are continuously being afforded for use
- TCA managed in an on-demand manner
  - Controls are reviewed or implemented before use
- TCA managed by a party other than the Responsible Entity
  - Controls are reviewed, implemented, or mitigated before use

Methods

Prohibit the use of RM or TCA to mitigate the risk of the introduction of malicious code

- The plan must document the methods used to prohibit the use of TCA or RM, either managed by the Responsible Entity or managed by a party other than the Responsible Entity
  - Administrative, physical, or technical controls

Methods

TCA managed by the Responsible Entity

- Antivirus software, including manual or managed updates of signatures or patterns, application whitelisting, or other method(s).
  - Other methods must achieve the objective of mitigating the risk of the introduction of malicious code.

slido

How often are TCA managed by a third party connecting to your low impact BES Cyber Systems?

ⓘ Start presenting to display the poll results on this slide.

Methods

TCA managed by a party other than the Responsible Entity.

- The Responsible Entity must review one or more of the party's method(s) before connecting the TCA.
  - Antivirus update process and level, application whitelisting, live operating system and software executable only from read-only media, system hardening, and other methods to mitigate the introduction of malicious code.
  - Determine whether any additional mitigation actions are necessary and implement the actions.

Methods

The Responsible Entity must decide what method(s) to use to detect and mitigate malicious code on Removable Media before use.

- The method used to detect malicious code cannot be a BES Cyber Asset that is part of a BES Cyber System.

Cybersecurity Plan Implementation

The Responsible Entity must **implement the methods** as documented in the TCA and RM cybersecurity plan(s) for its low impact BES Cyber Systems.

Example Implementation Artifacts

CIP Exceptional Circumstances (CEC)

- Dated report or documents, such as forms or templates with:
  - Description of the situation which triggered the CEC
  - Beginning and end date of CEC
  - BES assets and associated low impact BCS
  - Purpose for declaring the CEC
  - Any actions (security measures) taken during or after the event(s)
    - Such as scanning affected Cyber Assets for malicious code

Example Implementation Artifacts

Security control checklist or system generated evidence from a workflow identifying the security controls reviewed before RM or TCA use

- TCA/RM unique ID number
- Description of use
- Authorization for use
- Antivirus solution used, including version
  - Software, patterns, or signatures were verified as being up to date
- Confirmation of no detected malicious code/malware
  - System or device security scan or assessment results
- Network restriction controls
- Start and end dates of TCA/RM connection

Example Implementation Artifacts

- Group Policy Object(s)
- Whitelisting
  - Software
  - Ports and Services
- Running device configuration(s)
  - Antivirus/Malware including version
  - Manual or managed updated signatures or patterns installed
- System hardening method(s)
  - Log reviews or alerting
  - Master or base images
  - Administrative or technical controls

Example Implementation Artifacts

Specific to TCA managed by a party other than the Responsible Entity

- Documentation from change management systems, electronic mail, or procedures that document a review of the installed antivirus update level
- Memoranda, electronic mail, system documentation, policies, or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of operating systems, or system hardening performed by the party other than the Responsible Entity
- Evidence from change management systems, electronic mail, or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable

<Public>

TCA & RM SECURITY CHECKLIST

Device Type	TCA
Device ID	Device ID: UAT012_Palms
Authorized User	Jennifer Salisbury
Connection Date	10/10/2024
Location of Use	Palms Substation
Description of Use	Update SEL Firmware
Disconnection Date	10/10/2024

Third Party Device Type	N/A
Third Party Device ID	N/A
Third Party Company Name	N/A

Methods	Review Assessment	Date Reviewed	Reviewer Name
[Name of Antivirus] [Include version]	Authorized software installed and current.	10/8/2024	J.Bright
Signature/Pattern Status [Date of last install]	Latest signatures installed as of 9/3/2024.	10/8/2024	N/A
Network Restrictions	Wi-Fi and Blue tooth disabled. Guest account disabled.	10/10/2024	H.Watts
Operating System [Include version]	OS and software are current.	10/8/2024	J.Bright
EDR Solution [Include version]	Current. Reviewed last 10 days of activity, no threats.	10/8/2024	J.Bright
Contract/Service Level Agreement	N/A	N/A	N/A
Other Methods as Needed	No unauthorized software or malicious code detected. Attached scanned results and running config report.	10/10/2024	H.Watts

Date of Authorization ___10/10/2024_____

Authorized by ___H.Watts_____

<Public>

TCA & RM SECURITY CHECKLIST

Device Type	RM
Device ID	Device ID: MED001
Authorized User	Jennifer Salisbury
Connection Date	10/11/2024
Location of Use	Palms Substation
Description of Use	Retrieve configuration settings for backup.
Disconnection Date	10/11/2024

Third Party Device Type	N/A
Third Party Device ID	N/A
Third Party Company Name	N/A

Methods	Review Assessment	Date Reviewed	Reviewer Name
[Name of Antivirus] [Include version]	Scanned RM using authorized software and device TCA ID: UAT012_Palms	10/11/2024	J.Bright
Signature/Pattern Status [Date of last install]	TCA ID: UAT012_Palms used to scan RM had current signatures installed as of 9/03/2024.	N/A	N/A
Network Restrictions	N/A	N/A	N/A
Operating System [Include version]	N/A	N/A	N/A
EDR Solution [Include version]	N/A	N/A	N/A
Contract/Service Level Agreement	N/A	N/A	N/A
List Other Methods as Needed	No malicious code detected. Attached scanned results.	10/11/2024	J.Bright

Date of Authorization ___10/11/2024_____

Authorized by ___H.Watts_____

<Public>

TCA & RM SECURITY CHECKLIST

Device Type	N/A
Device ID	N/A
Authorized User	Jane Doe, Contractor
Connection Date	10/13/2024
Location of Use	Palms Substation
Description of Use	Scheduled Relay Maintenance Work Order #2024210
Disconnection Date	10/13/2024

Third Party Device Type	TCA
Third Party Device ID	SN#01234567891011
Third Party Company Name	Bulb LLC

Methods	Review Assessment	Date Reviewed	Reviewer Name
[Name of Antivirus] [Include version]	AV software installed and current. Client conducted scan for malicious code, none detected.	10/11/2024	J.Bright
Signature/Pattern Status [Date of last install]	Last update 9/25/2024	N/A	N/A
Network Restrictions	Wi-Fi and Blue tooth disabled. Guest account disabled. Installed network port blocker.	10/13/2024	H.Watts
Operating System [Include version]	OS version current.	N/A	N/A
EDR Solution [Include version]	N/A	N/A	N/A
Contract/Service Level Agreement	SLA on file is current. Client addendum for security controls executed on 1/1/2020.	N/A	N/A
Other Methods as Needed	Reviewed client vulnerability assessment for TCA dated 10/1/2024. No threats detected.	10/11/2024	J.Bright

Date of Authorization ___10/13/2024_____

Authorized by ___H.Watts_____

slido

Does your entity have a method to track the use of TCA or RM connected to your low impact BCS?

ⓘ Start presenting to display the poll results on this slide.

Cybersecurity Plan Recommendations

- How your entity manages TCA
  - Ongoing, on-demand, or a combination of both
- The acceptable use of TCA and RM
  - Maintenance testing, software updates, trouble shooting, configuration changes, vulnerability assessments, data transfer or storage, etc.
- Controls used to ensure TCA or RM is not connected for 30 consecutive calendar days or longer
- How to handle the use of TCA or RM for CIP Exceptional Circumstances
  - Pre or post scanning for malicious code of the devices or systems the RM or TCA was connected to
- Review the plan(s) at least annually or as needed due to changes in technology, methods, or threats

Implementation Recommendations

- Manage an accurate inventory of TCA and RM used to connect to low impact BES Cyber Systems
- Conduct periodic case studies to determine the use of TCA and RM managed by your entity or another party
- Conduct internal or third-party audits to ensure the methods are effective and being implemented as documented
  - TCA managed by the entity
  - TCA managed by a party other than the Responsible Entity
  - RM connected to a low impact BES Cyber System

Implementation Recommendations

Specific to TCA managed by a party other than the Responsible Entity

- Using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014
  - "*General Cybersecurity Procurement Language*" and "*The Supplier's Life Cycle Security Program*" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls

General Recommendation

- Stay connected and be involved
  - NERC Balloting and Commenting
  - WECC and NERC webinars and outreach events
  - WECC internal controls guidance and compliance failure points
  - Questions on new or revised CIP Reliability Standard Requirements questions
    - cip@wecc.org
    - CIP-003-9

References

- NERC One-Stop Shop (Compliance Monitoring & Enforcement Program)
  - https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx
- WECC compliance information
  - https://www.wecc.org/program-areas/compliance/compliance-united-states
  - https://www.wecc.org/program-areas/compliance/compliance-british-columbia
- NERC Balloting and Commenting
  - https://www.nerc.com/pa/Stand/Pages/Balloting.aspx
- Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014
  - http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

WECC

Electric Reliability and Security for the West

www.wecc.org