TEXAS RE

CIP-003-8 Section 5

Jason Georgoulis
CIP Cyber and Physical Security Analyst II

August 1, 2025

CIP Themes and Lessons Learned

Observations for Low Impact

Limited training	Insufficient understanding of environment	Challenges in implementing effective Transient Cyber Asset (TCA) plans

CIP-003-8 R2 Section 5

TCAs Managed by Responsible Entity

- Antivirus software
- Application whitelisting
- Other methods to mitigate the introduction of malicious code

TCAs Managed by a Third-Party

- Review of antivirus level
- Review of antivirus process
- Review of application whitelisting
- Review of live operating system and software from read-only media
- Review of system-hardening
- Other methods to mitigate the introduction of malicious code

Removable Media (RM)

- Methods to detect malicious code on Removable Media
- Mitigation of the threat of detected malicious code

TCA and RM Mitigation Strategies

MITRE ATT@CK Mitigations

ID	Mitigation	Description
M0949	Antivirus/Antimalware	Install anti-virus software on all workstation and transient assets that may have external access, such as to web, email, or remote file shares.
M0947	Audit	Integrity checking of transient assets can include performing the validation of the booted operating system and programs using TPM-based technologies, such as Secure Boot and Trusted Boot. [3] It can also include verifying filesystem changes, such as programs and configuration files stored on the system, executing processes, libraries, accounts, and open ports. [4]
M0941	Encrypt Sensitive Information	Consider implementing full disk encryption, especially if engineering workstations are transient assets that are more likely to be lost, stolen, or tampered with. [5]
M0930	Network Segmentation	Segment and control software movement between business and OT environments by way of one directional DMZs. Web access should be restricted from the OT environment. Engineering workstations, including transient cyber assets (TCAs) should have minimal connectivity to external networks, including Internet and email, further limit the extent to which these devices are dual-homed to multiple networks. [6]
M0951	Update Software	Update software on control network assets when possible. If feasible, use modern operating systems and software to reduce exposure to known vulnerabilities.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Networking devices such as switches may log when new client devices connect (e.g., SNMP notifications). Monitor for any logs documenting changes to network connection status to determine when a new connection has occurred, including the resulting addresses (e.g., IP, MAC) of devices on that network.
DS0029	Network Traffic	Network Traffic Flow	Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) may be helpful in identifying transient assets.

NIST Control Examples

MALICIOUS CODE PROTECTION

Control:

a. Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more): endpoint; network entry and exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; take* [*Assignment: organization-defined action*]]; and send alert to [*Assignment: organization-defined personnel or roles*] in response to malicious code detection; and

PTER THREE PAGE 334

SP 800-53, REV. 5 SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

TCA & RM Internal Controls

- Inventory Database
- Port Blocking
- Alerting
- Training
- Chain of Custody
- Comprehensive TCA & RM Authorization Forms

TEXAS RE
Ensuring electric reliability for Texans