CIP-010-2
Configuration Management and Vulnerability Assessment

Wayne Lewis
3/24/15
Configuration Change Management and Vulnerability Assessment – CIP-010-2

Purpose

• To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.
Configuration Change Management
Table R1

- Part 1.1 - Develop a baseline configuration, individually or by group, which shall include the following items:
  
  1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
  1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
  1.1.3. Any custom software installed;
  1.1.4. Any logical network accessible ports; and
  1.1.5. Any security patches applied.

- Identifies a change management process to be invoked
- Added baseline requirement to facilitate change management.
- Custom software is any additional software intentionally installed, e.g., scripts developed for local entity functions, or software developed for a specific task or function for the entity’s use.
- Doesn’t require identification of some minor software, e.g., notepad, calculator, DLL, device drivers that are included in an OS package as commercially available.
Configuration Change Management

Table R1

- Part 1.2 - Authorize and document changes that deviate from the existing baseline configuration.

- Part 1.3 - For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

- Track changes, update baseline.
Configuration Change Management

Table R1

- Part 1.4 - For a change that deviates from the existing baseline:
  
  - 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
  
  - 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
  
  - 1.4.3. Document the results of the verification.

- CIP-007-3 R1 test procedures are now implied in meeting requirement
- Explicitly defines CIP-005 and CIP-007 security controls
- Before the change, identify and afterwards verify those security control(s) that could be affected by the baseline configuration change
- No adverse effects on those controls after change
Configuration Change Management

Table R1 (High Impact BES Systems)

- Part 1.5 - Where technically feasible, for each change that deviates from the existing baseline configuration:
  - 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
  - 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

- Important to note EACH* change from the baseline
- If test environment is used, describe ANY* differences
- If on production, need a method to minimize adverse effects
Configuration Change Management

Table R1 (High Impact BES Systems)

• **FAQ** - If the vendor of a system, tests and verifies that patches are compatible with their system, up to and including all support components of the system, does that vendor testing meet the requirements of CIP-010-1 or will further testing at the facility be necessary before the patch is installed?
  - Depends on how closely the vendor has simulated the entity’s environment.
  - Must account for all of the customizations the entity has installed.
  - Does the vendor’s hardware match the entity’s hardware?
  - Is the vendor’s testing representative of the entity’s production environment?
  - Must document and account for deviations where they exist.
  - If entity is not running the current release version, whether or not customized, cannot rely upon the vendor unless the vendor can demonstrate that the Responsible Entity’s software version, including any customizations, was tested at the factory.
  - Vendor testing should be focused on addressing CIP Standards requirements for testing and not simply on functional testing.
  - Maintenance contracts with the vendor should specify what the vendor is testing.
  - Vendor needs to provide documentation of the testing to the customer in order to demonstrate compliance.
Configuration Monitoring
Table R2 (High Impact BES Systems and their associated EACMS, PCA)

• Part 2.1 –Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

- A specific requirement for once a month (35 days) review of malicious or intentional changes (automated or manually)
- Investigate unauthorized changes
Vulnerability Assessments

Table R3

• Part 3.1 – At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

• Paper (see guidelines/technical basis and NIST SP800-115)
  – network discovery - review of network connectivity to identified EAP to the ESP
  – port and service identification - look for all ports and services and appropriate business justification
  – vulnerability review - rule set reviews, default accounts, passwords, and network management community strings
  – wireless review - a review of common wireless networks and their controls to effect BES Cyber Systems comm.
Vulnerability Assessments

Table R3

- Part 3.1 – At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

- Active (see guidelines/technical basis and NIST SP800-115)
  - network discovery - active discovery tools for devices
  - port and service identification – active discovery tools, e.g., nmap
  - vulnerability review - live vulnerability scanning tools
  - wireless review - wireless scanning tools
Vulnerability Assessments
Table R3 (High Impact BES Systems)

- Part 3.2 – Where technically feasible, at least once every 36 calendar months:
  - 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and
  - 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

- If test environment used, identify differences
- If production is used, minimize adverse effects
- If a test environment is not available, and entity believes it can not minimize adverse effects, then entity must file a TFE.
Vulnerability Assessments

Table R3 (High Impact BES Systems and their associated EACMS, PCA)

- Part 3.3 – Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

- Active VA for introduction of new Cyber Assets
- Exception for CIP Exceptional Circumstances
- Exception for like replacements with baselines that model an existing baseline of the previous or existing other Cyber Assets
Vulnerability Assessments
Table R3

• Part 3.4 – Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of and remediation or mitigation action items.

- Results and Action plans of findings
- Define a planned date of completion and status for those findings
Transient Cyber Asset & Removable Media Protection - R4 (pending regulatory approval)

- Transient Cyber Assets and Removable Media

These requirements have been approved by the NERC BOT and are pending regulatory approval. They are very specific and include considerable additional guidance in the “Guidelines and Technical Basis” section of the standard document.
Transient Cyber Asset & Removable Media Protection - R4 (pending regulatory approval)

• **Transient Cyber Asset**
  A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is 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. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

• **Removable Media**
  Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.
Transient Cyber Asset & Removable Media Protection - R4 (pending regulatory approval)

• R 4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

  - Standard specifies in Attachment 1 the minimum requirements for documented plan(s) for Transient Cyber Assets and Removable Media.
Transient Cyber Asset & Removable Media Protection - R4

• Measures 4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

- Standard’s measures provides a number of specific examples of evidence in Attachment 2.
- If Transient Cyber Asset(s) or Removable Media are not used, evidence of this fact is required, e.g., a policy.
Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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.

- Evidence can be included as part of the authorization documentation of the TCAs.
- Allows an on-demand management approach prior to use.
Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

- **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;
  - 1.2.2. Locations, either individually or by group; and
  - 1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

- Transient Cyber Assets must be authorized, e.g., similar to CIP-004.
Transient Cyber Asset & Removable Media Protection - R4  Attachment 1

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

• From the “Guidelines and Technical Basis” for CIP-010-2 R4
  “1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited.”
Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

- **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.

- Transient Cyber Assets must be patched similar to CIP-007 R2. Note “per Transient Cyber Asset capability).
Transient Cyber Asset & Removable Media Protection - R4  Attachment 1

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

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.

- Transient Cyber Assets must be protected from malicious code similar to CIP-007 R3. Note “per Transient Cyber Asset capability” requirement.
Transient Cyber Asset & Removable Media Protection - R4  Attachment 1

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

• 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.
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.

- Third parties must provide documentation of their compliance.
Transient Cyber Asset & Removable Media Protection - R4 Attachment 1

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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.

- Third parties must provide documentation of their compliance.

3/27/2015
Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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.

- Other parties must provide documentation of their compliance.
- If other party’s actions are deficient, Responsible Entity is required to complete the mitigations prior to connecting their devices to an applicable system.
Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

- 3.1.1. Users, either individually or by group or role; and
- 3.1.2. Locations, either individually or by group.

- Removable Media must be authorized, e.g., similar to CIP-004.
Section 3. Removable Media

3.2. **Malicious Code Mitigation**: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

- 3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

- 3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.
Questions