



Better Practices to Provide Reasonable Assurance of Compliance with the CIP Standards, Part 2

David Cerasoli, CISSP
Manager, CIP Audits
October 30, 2018

Disclaimer

The goal of this webinar is to share practices that can help provide reasonable assurance of compliance with the CIP Standards. However,

implementing these practices does not guarantee that you will be in compliance with the CIP standards.

Today we will cover some general better practices as well as practices for CIP-005, CIP-007 and CIP-010, which are based on our experiences from over 23 onsite CIP Version 5 audits since July 2016.

Although questions will not be accepted during the webinar, you are encouraged to send any questions to cip@npcc.org.

An announcement with a link to these slides will be posted on NPCC's home page later today.

Reliability Standard Audit Worksheets (RSAWs)

After completing the RSAWs for each in-scope CIP standard and requirement, you should **consult the Compliance Assessment Approach section** to:

- Verify RSAW narratives and supporting evidence address each item
- Prepare SMEs for the types of questions they may be asked
- Gain a better understanding of the audit approach for each standard

Managed Service Providers

If you use managed service providers to manage or host applicable Cyber Assets, then **consider obtaining from your providers any information** that may be required to support your compliance program **well in advance of your next CIP audit**. Such information may include:

- Network diagrams and configuration information
- Interactive Remote Access procedures
- System configurations and baselines
- Change control procedures
- Patch management program
- Malicious Code controls
- Logging and alerting
- User authorizations, access controls and accounting
- Vulnerability management
- Information protection program
- Physical security program

This type of support is often documented in a Service Contract SLA

CIP-005-5, Part 1.1 ESP Diagrams

CIP-005-5 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5, Part 1.1

ESP Diagrams

If you use diagrams to support compliance with Part 1.1, then **ensure the diagrams are current to the end of the audit period and contain a legend**. Also, consider including the following on your diagrams:

- ESP Boundaries
- All Applicable cyber assets
- EAPs and EACMS
- Non-routable protocols entering/exiting the ESP
- Dial-up connections
- VPN Tunnels for extended ESPs (CIP-006-6, Part 1.10)
- IDS taps/span ports
- Revision history

CIP-005-5, Part 1.2

Correctly Identify EAPs

CIP-005-5 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5, Part 1.2

Correctly Identify EAPs

NERC Glossary of Terms (July 7, 2018):

Electronic Access Point	Project 2008-06 Order 706	EAP	11/26/2012	11/22/2013	7/1/2016	A Cyber Asset <u>interface</u> on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
-------------------------	---	-----	------------	------------	----------	---

Examples of an EAP include:

- Firewall port
- Switch port
- Router port
- Virtual Network Interface Controller

Typically an EAP is part of an EACMS. For example, an entire firewall may be an EACMS, while one or more of the firewall's ports may be an EAP.



CIP-005-5, Part 1.3

Thoroughly Document Permissive Access Permissions

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

CIP-005-5, Part 1.3

Thoroughly Document Permissive Access Permissions

If your inbound or outbound access permissions ***allow large ranges of source addresses***, destination addresses or protocols then you should:

- Document the reason for granting access
- Explain the reason for the “permissiveness”
- Provide supporting vendor documentation to substantiate the need for such a permissive rule

CIP-005-5, Part 1.5

Use of IDS/IPS to support CIP-007-6 R3 Malicious Code Prevention

CIP-005-5 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-5, Part 1.5

Use of IDS/IPS to support CIP-007-6 R3 Malicious Code Prevention

If you use an IDS or IPS as a control to support CIP-007-6, R3 Malicious Code Prevention then you should:

- Document the control as it relates to CIP-007-6, R3
- Explain how updates are tested and installed (CIP-007-6, Part 3.2)
- Explain how alerts are handled

CIP-007-6, R3

Malicious Code Prevention

CIP-007-6 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6, R3

Holistic Approach to Malicious Code Prevention

Adopt a **holistic approach** that considers **all controls** used to **deter, detect or prevent malicious** code, not only the fact that a specific Cyber Asset is not capable of running anti-malware services. Examples include:

- White-listing solutions
- Network isolation techniques
- Intrusion Detection/Prevention (IDS/IPS) solutions
- Internal firmware validations
- Device hardening

We strongly recommend consulting the Guidelines and Technical Basis section of the Standard for more information on controls to consider.

CIP-010-2, R1

Baseline development

CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2, R1

Baseline development

This requirement includes processes used to **develop and maintain baselines**.

- Document the steps taken to develop new baselines
- Consider using unique Cyber Asset types where baselines are created and maintained individually
- Technical documentation from your vendor is often a good source of information

CIP-010-2, Part 3.1

Compare Work Performed to Documented Process

CIP-010-2 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2, Part 3.1

Compare Work Performed to Documented Process

Ensure that **work performed** during the vulnerability assessment **covers all items in your documented vulnerability assessment process**. To that end:

- When applicable compare vendor provided Scope-of-Work to final reports
- Confirm that various units and groups within your company are consistently implementing the documented policy or process and getting consistent results

We strongly encourage you to consult the Guidelines and Technical Basis for CIP-010-2 R3

CIP-010-2, Part 3.4

Clearly Identify Assessment Findings in Associated Action Plans

3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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 any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
-----	---	---	---

CIP-010-2, Part 3.4

Clearly Identify Assessment Findings in Associated Action Plans

Ensure that any vulnerability assessment findings are clearly identified in the associated action plans.

- Considering numbering or indexing action plans items for easier cross-reference with vulnerability assessment findings
- Identify action plan activities that address multiple vulnerability assessment findings
- Ensure any documentation that supports the completion of action plans (ex: change tickets or work orders) is available



CIP-010-2, R4, Attachment 1, Section 1.1 Ongoing vs. On-demand Management of TCAs

CIP-010-2 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

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.

CIP-010-2, R4, Attachment 1, Section 1.1

Ongoing vs. On-demand Management of TCAs

Clearly identify how Transient Cyber Assets (TCA) are being managed in your TCA plan. TCAs can be managed in the following two ways:

- **Ongoing** – Preauthorized TCAs that are continuously managed/compliant and may be used for approved TCA functions at anytime
- **On-demand** – Validation of the security status/compliance of a Transient Cyber Asset prior to connecting it to an ESP, or an applicable BES Cyber Asset/System

*The standard **allows for a combination of ongoing and on-demand management** depending upon business process. **Pick the method or combination of methods that works best for you.***

Thanks for your time!

**Feel free to contact cip@npcc.org
with any questions you may have.**