

NPCC Compliance Monitoring Team Classroom Session

John Muir - Director, Compliance Monitoring
Jacqueline Jimenez - Senior Compliance Engineer
David Cerasoli, CISSP - Manager, CIP Audits

Compliance Monitoring

- Team Member Introductions
- Audit Process
- Audit Preparation Insights
- Update on CIP-003-7 Implementation
- Open Forum for Questions

Audit Process

John Muir
Director, Compliance Monitoring

Audit Process

Day 0 – Notification Letter with Pre-Audit Survey and Data Request

~Day 10 – Initial Audit Briefing Conference Call

Day 30 – Pre-Audit Submittal and Data Request due

Day 90 – RSAWs and Evidence submittal due (End Day of Audit Period)

Days 90 – 120 - Auditors review submittal and send requests for additional evidence as necessary.

Day 120 – Start of on-site audit or expected completion date of off-site audit

Day 150 – Draft Report issued -2 weeks allowed for comments

Day 165 – Comments due

Day 170 – Final Report Issued

Refer to Our March 23, 2018 Presentation available on the NPCC Web site.
Compliance / Documents / Compliance Webinars

Audit Preparation Insights

Jacqueline Jimenez
Senior Compliance Engineer

Audit Submittal Issues

- Only evidence submitted is an attestation.
- Overload of non-specific evidence - data dumping.
- Specific evidence documents identified, but are not annotated.
- Incomplete narrative when filling out RSAWs.

O&P Audit Submittal Issues

- PRC-005
 - R3. – In order to verify maintenance intervals are being respected, auditors may request evidence from before the start of the audit period to get the previous maintenance and the current maintenance dates and records to verify the intervals.

O&P Audit Submittal Issues

- When providing PRC-005 evidence, do not repeat the same information for each relay provided that is general, but needed information. Provide that information once, i.e. cover page with all of the common statements, then provide the individual test records annotated.
- Provide clear identification of records to correlated sample set spreadsheet.

O&P Audit Submittal Issues

- Provide one-line diagrams (GO, GOP, DP) clearly identifying the demarcation point.

Examples

- Annotated evidence

- **Good:**

- The section is highlighted with a word bubble of the requirement it is satisfying.

4.3. Tested Contingencies

Table 3 Voltage Contingency Definitions lists the contingencies that were evaluated for each configuration studied.

Table 3 Voltage Contingency Definitions

Contingency	ID	Elements lost	Line IDs	Voltage (kV)

FAC-014-2 R1
The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology.

Examples

- Annotated evidence

- **Bad:**

- Providing a document with no highlighting to identify the section to be reviewed or references to the exact page.
 - This can result in the auditors asking follow-up questions.

Examples

- PRC-005 submittal
 - **Good:**
 - Relay test records where all pertinent information is highlighted.
 - Spreadsheet containing data by substation, that provided explanation of the spreadsheet and very clear column headings, i.e. component, description, manufacturer/model, operates/trips, test dates (last, current, future)

Examples

- PRC-005 submittal

- **Bad:**

- Relay test record with 313 pages of evidence. No pertinent information highlighted or annotated.
 - Spreadsheet with no column headings or test dates provided.

Examples

- Non-applicable requirement
 - **Good:**
 - Entity policy, procedure or document which supports the non-applicability of the requirement.
 - Another entity's (RC, TOP, etc.) policy or procedure that corroborates the non-applicability of the requirement.
 - In conjunction with other documentation, an attestation.

Examples

- Non-applicable requirement
 - **Bad:**
 - Stating the requirement is not applicable without any supporting evidence or reason explaining why the requirement is not applicable.

CIP-003-7, Attachment 1

Sections 2, 3 and 5

David Cerasoli, CISSP
Manager, CIP Audits

This film has been modified from its original version. It has been edited to run in the time allotted. Please refer to the actual CIP-003-7 standard and its implementation plan before making any compliance decisions.

CIP-003-7 Compliance Timeline

- CIP-003-7 and its implementation plan were approved by FERC on April 19, 2018.
- The effective date of CIP-003-7 is January 1, 2020.
- You are still required to comply with all of CIP-003-6 except Att. 1, Sections 2 and 3.
- You now have until January 1, 2020 to comply with CIP-003-7, Att. 1, Sections 2 and 3.
- LERC and LEAP will be retired immediately prior to the effective date of CIP-003-7.

Summary of CIP-003-7, Attachment 1

Responsible entities with at least ***one low impact BES Cyber System*** are required to implement a cyber security plan for its low impact BES Cyber System that include all five sections in Attachment 1.

Section 1. Cyber Security Awareness

Section 2. Physical Security Controls

Section 3. Electronic Access Controls

Section 4. Cyber Security Incident Response

Section 5. TCA and Removable Media Malicious Code Risk Mitigation

Attachment 1, Cont.

- You are not required to maintain a list of low impact BES Cyber Assets, but we strongly suggest that you do.
- You are allowed to apply existing policies, procedures, and processes for your high or medium impact BES Cyber Systems to your low impact BES Cyber Systems.

Mapping of Att. 1 to the other CIP Standards

Section 1. Cyber Security Awareness Plan

- CIP-004-6, R1 - Security Awareness

Section 2. Physical Security Controls

- CIP-006-6, R1 - Physical Security Plan, Access Controls

Section 3. Electronic Access Controls

- CIP-005-5, R1 - Electronic Security Perimeter

Section 4. Cyber Security Incident Response

- CIP-008-5, R1 - Cyber Security Incident Response Plan

Section 5. Transient Cyber Assets (TCAs) and Removable Media Malicious Code Risk Mitigation

- CIP-010-2 Attachment 1 - Plans for TCAs and Removable Media

What's new in CIP-003-7 Attachment 1?

Section 2 – Physical Security Controls

LEAP was removed, but you are still required to control physical access to your low impact BES Cyber Systems and the Cyber Assets that provide electronic access controls.

Section 3 – Electronic Access Controls

LERC and LEAP have been removed. However, you are still required to control electronic access and protect Dial-up connections, except where communication is used for time-sensitive protection or control functions between Intelligent Electronic Devices.

Section 5 - TCA and Removable Media Malicious Code Risk Mitigation

This new section will require you to mitigate the risk of introduction of malicious code to low impact BES Cyber Systems from TCAs and Removable Media.

Section 5, Cont.

You can choose whether to manage your TCAs in an ongoing or on-demand manner.

- Ongoing is active management
- On-demand is immediately prior to connecting a TCA to your BES Cyber System

Section 5, Cont.

3rd party TCAs will need to be checked for use of one or more of the following before they are connected to your BES Cyber Systems:

- 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 the introduction of malicious code.

Section 5, Cont.

You will need a method for detecting and mitigating the threat of detected malicious code for Removable Media.

**What might NPCC Auditors ask for
auditing Sections 2, 3 and 5?**

General Requests

1. Your Cyber Security Plan
2. List of BES Cyber Systems / Assets
3. Electronic Access Controls device configuration
4. We may want to visually inspect the BES Cyber System, associated Cyber Assets and the physical locations where they reside.

Section 2 – Physical Security Controls

- Does your Cyber Security Plan cover physical security controls for your low impact BES Cyber Systems and associated access controls?
- Describe your rationale for determining who needs physical access to your BES Cyber System locations?
- Where are the low impact BES Cyber Systems and their associated electronic access controls located?
- Did you actually implement the controls documented in your Cyber Security Plan?

Section 3 – Electronic Access Controls

- Does your Cyber Security Plan cover electronic access controls for your low impact BES Cyber Systems?
- Is there routable connectivity to your BES Cyber Systems?
 - If yes, how is access control performed for inbound and outbound access?
- Is there Dial-up connectivity to your BES Cyber Systems?
 - If yes, are there controls to authenticate all Dial-up Connectivity?
- Have the controls documented in your Cyber Security Plan actually been implemented?

Section 5 – TCAs and Removable Media

- Does your Cyber Security Plan cover TCAs and Removable Media?
- Do you actually have any TCAs, 3rd party TCAs and/or Removable Media?
 - If yes, how do you keep track of TCAs and Removable media, e.g., spreadsheet or database?
- Are you managing your TCAs in an ongoing or on-demand manner?
- What sort of malicious code prevention, detection and/or mitigation tools or methods are you using?

Questions

NPCCCompliance@NPCC.org