
RELIABILITY
& SECURITY
Workshop–San Diego, CA
OCTOBER 31–NOVEMBER 1

Audit Success

Industry Panel

October 31, 2023

Stacia Carron, Manager, Entity Monitoring, WECC

Casey Jones, Manager, NERC CIP Compliance, NV Energy

Hans Schmid, Senior NERC CIP Specialist, NV Energy

Jennie Wike, NERC Compliance Lead, Tacoma Power

Jessica Lopez, Regulatory Compliance Advisor, Arizona Public Service

What Will You Learn and Why it Matters

- Learn from industry about best practices for:
  - Narrative preparation
  - Evidence packaging
  - Working across multiple platforms
- Best practices help you succeed at audit

Audit & Readiness Assessment

- Audit preparation starts six to 18 months before the start of the audit
- Assign Subject Matter Experts (SMEs) audit tasks
- Maintain Regional evidence tools (CIP Evidence Request Tool, O&P Evidence Spreadsheet)
- Three potential options for mock audits and readiness assessments:
  - Internal Peers (SME to SME)
  - Third Party Consultant
  - Industry External Peers

Audit Logistics

- Reserve conference rooms for meetings, training sessions, mock interviews and audit interviews
- Test conference room technology and document settings for quick reference
- Coordinate with SMEs and management to ensure their availability during the audit engagement
- Communicate and plan with WECC regarding site visits
- Participate in the WECC workshops and WICF audit panels for latest information regarding audit activities, expectations, and lessons learned
- Document lessons learned throughout the audit engagement

Communication Plan

- Compliance SharePoint site used for storing audit documentation and accessible to approved SMEs
- Communicate to all applicable stakeholders (SMEs, senior leadership, legal, etc.)
- Establish communication milestones

Interview Preparation

- Practice interviews as part of a mock audit
- Identify primary and backup SMEs for in-scope Standards
- Provide training to prepare SMEs, promote comfort in interview settings, and familiarize with digital resources
- Use the WECC Controls Guidance and Common Failure Points to prepare for potential internal control questions
- Prepared for remote, hybrid or on-site interview environments

Request for Information

- Assign a data request coordinator
- Train SMEs and their managers on the RFI process
- Create a template for RFI responses
- The process for completing RFI's was documented in a workflow prior to audit

Compliance Narrative & Evidence Collection

- Prepare compliance narratives and evidence in an ongoing manner
- Describe how you ensure compliance with the requirement and internal controls
- Compliance narratives are reviewed by a third party, compliance team, and legal
- Adapt RSAWs to fit into Align

The goal is to effectively demonstrate compliance and assist in reducing RFIs and interview questions.

CIP Evidence Request Tool

- Prepare the ERT one year in advance (anticipate the most current version)
- Provide a narrative file for each Level 1 and Level 2 requests
- After CIP ERT submission, expect L2 Request for Information within five days **or** reach out to WECC

Narrative File Example 1

- Example of a simple response to an ERT RFI (Level 1)

2023 CIP Audit – ERT Request CIP-006-R1-L1-01

Provide each documented physical security plan(s) that collectively includes all of the applicable requirement parts in CIP-006 R1.

Measures

The following evidence is presented which encompass both general and specific security plans.

- CIP Physical Access Controls Procedure.pdf
- Site Specific Security Plans.pdf

The **CIP Physical Access Controls Procedure** cites specifically the document(s) most applicable to each part of the standard on **pages 5-6**, and which sections of each document are best referenced to determine controls applicable to each part.

Narrative File Example 2

- Example of a more complex response to an ERT RFI (Level 2)

2023 CIP Audit – ERT Request CIP-010-R1-L2-03

For each Cyber Asset in Sample Set CA-L2-10, for the range of dates in SS-DATE-04, provide the following evidence for each change that deviated from the then-existing baseline configuration:

1. *The date of the completion of the change; and*
2. *The date the baseline was updated; and*
3. *Evidence that the baseline was updated to reflect the change.*

SS-DATE-04: **10/27/2021 – 10/28/2022**

Sample Set CA-L2-10

Index	Cyber Asset ID	Asset ID	Impact Rating
2	PCC 1 PACS	PCC 1	High
11	PCC 1 FEPS	PCC 1	High
21	PCC 1 Server	PCC 1	High
65	PCC 1 Workstation	PCC 1	High
84	PCC 2 FEPS	PCC 2	High
187	BUCC 1 FEPS	BUCC 1	High
220	Sub 1 Relay 1	Substation 1	Medium
250	Sub 1 Relay 2	Substation 1	Medium

Measures

For a change that deviates from the existing baseline configuration, NV Energy updates baselines configurations within 30 calendar days of completing the change.

From Sample Set CA-L2-10, Cyber Assets "PCC 1 Server" and "PCC 1 Workstation" had baseline changes during SS-DATE-04. Both are Tripwire enabled devices. The baselines for these assets are updated automatically through a daily scheduled task which pulls the device-level configurations. Table 1 details the date of installation for each change along with the date the baseline was updated. The baseline is updated during the next Tripwire scheduled task which reflects the updated device level configuration.

Evidence of installation and baseline updates are detailed in Table 1. **Baseline Evidence** details the Tripwire files that demonstrates the implementation of Cyber Asset change. **Baseline File – Evidence of Change** is a summary of changes for both assets. Screenshots for each change are taken from the daily Tripwire baseline file in which the change is first reflected. Excel files for each daily scan reflecting the change can be provided if requested.

Table 1: Installation of Change and Baseline Update

Cyber Asset ID	Patch Identifier	Install Date	Baseline Evidence	Date Baseline was Updated	Baseline File - Evidence of Change
PCC 1 Server	202110 Microsoft Updates (Security Only)	11/3/2021	Tripwire Baselines.xlsx	11/4/2021	PCC1SRV Change.pdf
PCC 1 Server	202111 Microsoft Updates (Security Only)	12/1/2021	Tripwire Baselines.xlsx	12/2/2021	PCC1SRV Change.pdf
PCC 1 Server	202110 Tripwire agent 8.8.3.4 _ Servers	11/17/2021	Tripwire Agent.xlsx	11/18/2021	PCC1SRV Change.pdf
PCC 1 Server	202112 Compliance Tool agent	12/15/2021	Tripwire Baselines.xlsx	12/16/2021	PCC1SRV Change.pdf
PCC 1 Server	202112 Microsoft Updates (Security Only)	1/5/2022	Tripwire Baselines.xlsx	1/6/2022	PCC1SRV Change.pdf
PCC 1 Server	202112 Microsoft Updates (Monthly Rollup)	1/5/2022	Tripwire KB5007260.xlsx	1/6/2022	PCC1SRV Change.pdf
PCC 1 Server	202201 Microsoft Updates (Monthly Rollup)	2/2/2022	Tripwire Baselines.xlsx	2/3/2022	PCC1SRV Change.pdf
PCC 1 Server	202201 Microsoft Updates (Security Only)	2/2/2022	Tripwire Baselines.xlsx	2/3/2022	PCC1SRV Change.pdf

Align & SEL Lessons Learned

- Review WECC Align training prior to audit
- Check Align and SEL access permissions
- Compliance narratives in Align vs. RSAWs
- Large files must be separated into multiple files in SEL
- Notify WECC when evidence is uploaded to SEL
- No major issues using Align and SEL, although, Align was down for maintenance for several hours during the audit

Trust, Relationship, Positive Interactions

- Audit Team Leads presented status for each Requirement in daily debrief meetings
- WECC provided sufficient time to respond to RFIs and was flexible when more time was needed
- Virtual demonstrations of in scope processes reinforced WECC's need to understand the entity's complete program
- Lunch with WECC team on site visits

Feedback to WECC

- A link to the NERC Post Audit Feedback Survey is included in Compliance Audit Preliminary Findings presentation at the end of every audit
- Is encouraged for all phases of audit
- Helps improve WECC processes

<Public>

WECC

Electric Reliability and Security for the West

www.wecc.org