NPCC, Inc.

How to prepare for CIP Audits

NPCC, Inc.

Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters' own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.

Auditors, can’t live without ‘em

CIP Auditors aren’t out to get ya!

Non-Compliance is no fun for anyone.

They're there to help you improve your cyber security posture.

The CIP Audit Process

- Formal Notification & Pre-audit Survey
- Pre-audit Questionnaire/RSAWs, Pre-audit submittal.
- Your Audit Team
- The Audit
  - Opening Presentations
  - Questions & Answers
  - Final Submittal (The Envelope)
  - Exit Presentation & Results

Formal Notification & Pre-Audit Survey

- Three months before the Audit, the formal notification is sent from NPCC along with the Pre-Audit survey.
- Formal notification of an audit will clearly indicate what requirements are being audited an over what time period.
- In addition to the auditable requirements, an assessment of other requirements and/or Technical Feasibly Exceptions (e.g. Part B) may be done.

Formal Notification & Pre-Audit Survey *continued*

Pre-Audit Survey

- Contact Info
- Your entities registered functions
- Logistical Info
- Confidentiality and Background Checks
- Organizational Profile
- Delegated Reliability Standard Requirements
- Additional Regional Questions (Compliance Culture)

Reliability Standards Audit Worksheets RSAWs

- Get them at
  NERC | Compliance | Resources
- Like getting to see all the questions well before the test.
- Use them as a road map to all your CIP documents.
- Make them part of your document change management. Not just something you do prior to an audit.

Pre-Audit RSAW Submittal

- Complete the RSAWs and gather supporting information.
- At this point, do not include sensitive information, but list those documents that are not included.
- Package the information electronically and submit to NPCC over secure FTP (20 days before Audit)

Evidence Data Hierarchy

- CIP Audit *YYYY Entity*
  - CIP-002
    - R1
      - RSAW CIP-002-1
      - Supporting Evidence
        - Risk Based Methodology for Identifying CA
    - R2
      - RSAW CIP-002-1
      - Supporting Evidence
        - List of Sensitive Documents Not Included
        - List of Critical Assets

For Pre-Audit Submittal

…and so on.

Your Audit Team

- Subject Matter Experts (SMEs)
- Same people who completed pre-audit RSAWs
- There is sufficient notice of an audit to schedule SMEs well in advance, bit if you must use alternates, have that person brought up to speed well before the audit.

Your Audit Team *continued*

- They must have the ability to query various systems and provide logs/reports to the auditors on demand.

- In the weeks prior to the audit, your SMEs should complete the Evidence Data Hierarchy by adding sensitive information that was omitted in the Pre-Audit submission.

Your Audit Team *continued*

- Like the pre-audit submission, RSAWs should hyperlink to supporting information.
- Have the information ready on at least two CDs or provide laptops for the auditors to use.
- If your SMEs are new to NPCC audits, do a practice run. There are also many consulting companies who offer mock audit services.

The Audit: Opening Presentations

- The lead auditor will open the audit process with introductions and an overview of the compliance audit process.
- The entity follows up with an…
  - Introductory Presentation
    (similar to the Pre-Audit Survey)
    - About your company
    - Operating characteristics
    - Your compliance framework
  - and a Technical Presentation
    - Your electronic security perimeter and access points.

The Audit: Questions & Answers

- The auditors will usually break into teams and tackle at least two standards at a time.

- Most of the answers the Auditor is looking for will be in your Evidence Data Hierarchy. The auditor will ask questions for clarification and may request logs and reports for proof of your adherence to the standard.

The Audit: Q & A *continued*

- Evidence that cannot be provided immediately is tracked in a spreadsheet by sub-requirement. Items are closed as the evidence is gathered to the satisfaction of the auditor.

- If possible have someone from your company always present in an observer role to assist SMEs with evidence tracking and to gather information that could improve audits in the future. (e.g. your primary compliance officer)

The Audit: Final Submittal (Envelope)

- The Evidence Data Hierarchy that was prepared before the audit along with other supporting evidence as requested by the Auditors during the Q & A process (both immediate and through the closing of items on the evidence tracking spreadsheet) forms the Final Submittal.

- The Final Submittal comprises of all the information that supports your adherence to the standards which were audited.

The Audit: Final Submittal (Envelope)

- This Final Submittal does not leave the site as it contains sensitive information.
- The Final Submittal is compressed (.zip file) and a digital hash is computed (e.g MD5). Both the CD/DVD and hash value are sealed in a TyVek envelope.
- The NPCC auditors sign the envelope which is then stored safely on-site until the next regular scheduled audit.
- The envelope may be opened on-site by NPCC to validate audit results prior to the next scheduled audit.

The Audit: Exit Presentation & Results

- The Auditors will make a presentation to your audit team of their preliminary findings.
- Your audit team will have an opportunity to complete an audit process feedback form (~ 10 questions).
- Both a public and non-public report will be produced in the coming weeks.

NPCC, Inc.

Q&A

Questions or Comments?