

Preparing for a successful CIP Audit

Val Ayers

Powerful Solutions Consulting Inc.

Audit Schedules

- Schedules are set by NERC
- Regional Enforcement
- Utilities register with NERC on the functions they perform BA,RC,TO,LSE.....
- CIP Audits are on-site audits
- Regions pre schedule year ahead
- No surprises

Preparation

- Regional sends notice to utility to notify that an audit is to be scheduled
- An audit package is sent to utility
- RSAWS (Reliability System Auditor Worksheets)
- List of CIP requirements to be included
- Utility has 60 days to return responses

Confidential

- A large portion of a submittal includes information that is very sensitive.
- No information is shared outside the audit team.
- Critical Assets and Critical Cyber Assets are not disclosed until on-site
- Auditor must have background checks, NERC training, and sign agreements

Documentation

- Policies, Procedures, Risk Assessment
- Personnel Background Checks
- Change Management
- Training programs
- Disaster and Backup plans
- Authority
- Revisions and effective dates

The Audit

- Currently taking about a week?
- How many people does it take ?
- NERC and FERC observers.
- Review submitted information them request supporting documentation and collaborating evidence.
- Interviews of SME

The Audit

- Tour of facility and computer room
- Review network configuration
- Security Systems
- Document Control
- “Culture of Compliance”

The Wrap UP

- No evidence leaves the premise
- All submittals and data requests must be handled during the on- site.
- The Lead auditor prepares and exit briefing with the findings and the presents to utility.
- Auditors can only report “possible violations”