CIP-10-2 Change Management

March 10, 2015

Steven Keller

Lead Compliance Specialist - CIP

skeller.re@spp.org · 501.688.1633

SPP Southwest Power Pool Regional Entity

CIP-10-2 BASICS R1 AND R2

What is CIP-010-2?

- The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems
- Understand what is on your system(s)
- Be aware of authorized or unauthorized changes to any and all BES Cyber Systems
- Baselines, Baselines, Baselines

V5 vs V3 for CIP-10-2 R1 and R2

- CIP-003-3 R6: Change Control and Configuration Management
- CIP-007-3 R1: Testing
- Requirement applies to all BES Cyber Assets within the identified BES Cyber System(s)

CIP-010-2 R1.1 Requirement

- **Develop a baseline configuration, individually or by group, which shall include the following items:**

  1.1.1. Operating System or firmware where no independent OS exits

  1.1.2. Any commercially available or open source application software intentionally installed

  1.1.3. Any custom software installed

  1.1.4. Any logical network accessible ports

  1.1.5. Any security patches applied

CIP-010-2 R1.1 Baseline Minimum

- **Five Basic required items to include in your baseline:**
  1. **OS Software or firmware**
  2. **Intentionally installed commercial and/or open source software**
  3. **Any custom applications**
  4. **Open logical network accessible ports**
  5. **Security patches that have been applied**

CIP-010-2 R1.2 Requirement

- Authorize and document changes that deviate from the existing baseline configuration

CIP-010-2 R1.2 Approach

- Who is authorized to approve changes?
- Who is allowed to make those changes?
- How will you document those changes?

- Do not allow the approver of the changes to be the one making the changes

CIP-010-2 R1.3 Requirement

- For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

CIP-010-2 R1.3 Approach

- Baseline should be updated 30 days after that patch was installed or software updated

CIP-010-2 R1.4 Requirement

- **For changes that deviate from existing baseline configuration:**

  1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

  1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and

  1.4.3 Document the results of the verification.

CIP-010-2 R1.4 Approach

- What are those controls?
- Controls for Windows vs. Unix vs. Cisco
- Verify all changes made to baseline are properly documented and approved
- What evidence do you have to show controls were tested and not adversely affected?

CIP-010-2 R1.5 Requirement

- **Where technically feasible for each change that deviates from the existing baseline configuration:**

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and

CIP-010-2 R1.5 Req. – Cont.

- **Where technically feasible for each change that deviates from the existing baseline configuration:**

1.5.2. Document the results of the testing and, if a test environment was used, the difference between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environment.

CIP-010-2 R1.5 Approach

- Applies to High Impact BES Cyber Systems
- If a test environment was used, must document the difference between test and production environments
- List those controls tested and document the results of those tests

CIP-010-2 R2.1 Requirement

- Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1).
- Document and investigate detected unauthorized changes

CIP-010-2 R2.1 Approach

- Monitor for changes at least once every 35 days
- What is the monitoring process? How do you ensure you do not miss the 35 day deadline?
- Logs, change tickets, or tracking sheets?
- Keep your records and know where they are kept
- Is there a file monitoring tool that can be used?