CIP v5 RSAW and Evidence

Lew Folkerth, PE, CISSP, CISA, GCFA
SPP RE CIP Workshop
June 2, 2015
Agenda

- **RSAWs**
  - The Role of the RSAW
  - Development Overview and Strategy
  - Organization and Structure
  - Navigation
  - Compliance Assessment Approach
  - Tips

- **Evidence**
  - Policy/Process/Procedure
  - Populations
  - Sample Sets
  - Sampling Strategies
  - Applicability
  - IRA and ICE Considerations
RSAW$s$
The Role of the RSAW

The RSAW is required in this part only
The Role of the RSAW

How the RSAW is Used

• Before an audit, RSAWs may be used by an entity to organize compliance efforts and prepare for compliance monitoring actions.

• During an audit, RSAWs are used as a tool to organize compliance evidence and to communicate an entity’s compliance approach to the audit team.

• During and after an audit, RSAWs are used by audit teams to organize, execute, and document a compliance assessment as part of the Entity Compliance Oversight Plan.
NERC/Region core development team
- Development began in early 2013
- Draft 1 had extensive evidence requests and guidance
- Based on comments, Draft 2 had evidence requests and most of the guidance removed

Advised by additional Region specialists

Posted four times for industry review/comment

Three meetings with 791 SDT

Final review by NERC legal staff

Final version posted 5/8/2015 for public use
RSAW Development Strategy

- One RSAW per Standard - TFE and CIP Exceptional Circumstance review embedded in the applicable Requirements
- One section per Part, rather than one section per Requirement
- Minimal guidance included
- In most cases, audit review is based on outcomes (actual work performed), rather than documentation
RSAW Structure

General Information

- Cover Page
- Findings Page
- Subject Matter Experts
- Page Footer
- Additional Information

Repeated for each Requirement:

- Text of Requirement and/or Part
- Question(s), if applicable
- Compliance Narrative
- Evidence Table
- Evidence Reviewed
- Compliance Assessment Approach
- Note(s) to Auditor, if applicable
Reliability Standard Audit Worksheet

CIP-002-5.1 — Cyber Security — BES Cyber System Categorization

This section to be completed by the Compliance Enforcement Authority.

| Audit ID: | Audit ID if available; or REG-NCRnnnnn-YYYYMMDD |
| Registered Entity: | Registered name of entity being audited |
| NCR Number: | NCRnnnnn |
| Compliance Enforcement Authority: | Region or NERC performing audit |
| Compliance Assessment Date(s): | Month DD, YYYY, to Month DD, YYYY |
| Compliance Monitoring Method: | [On-site Audit | Off-site Audit | Spot Check] |
| Names of Auditors: | Supplied by CEA |

### Applicability of Requirements

<table>
<thead>
<tr>
<th>BA</th>
<th>DP</th>
<th>GO</th>
<th>GOP</th>
<th>IA</th>
<th>LSE</th>
<th>PA</th>
<th>PSE</th>
<th>RC</th>
<th>RP</th>
<th>RSG</th>
<th>TO</th>
<th>TOP</th>
<th>TP</th>
<th>TSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- Text with blue background: Fixed text – do not edit
- Text entry area with Green background: Entity-supplied information
- Text entry area with white background: Auditor-supplied information
## Findings
(These sections to be completed by the Compliance Enforcement Authority)

<table>
<thead>
<tr>
<th>Req.</th>
<th>Finding</th>
<th>Summary and Documentation</th>
<th>Functions Monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>P1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P1.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P1.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td>P2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P2.3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req.</th>
<th>Areas of Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req.</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Req.</th>
<th>Positive Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Subject Matter Experts**
Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

**Registered Entity Response (Required; Insert additional rows if needed):**

<table>
<thead>
<tr>
<th>SME Name</th>
<th>Title</th>
<th>Organization</th>
<th>Requirement(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adam Jones</td>
<td>EMS Support Manager</td>
<td>EMS Support</td>
<td>R1, R2</td>
</tr>
<tr>
<td>Ben Smith</td>
<td>EMS Engineer</td>
<td>EMS Support</td>
<td>R1</td>
</tr>
<tr>
<td>Christine Taylor</td>
<td>Network Specialist</td>
<td>IT Networking</td>
<td>R2</td>
</tr>
</tbody>
</table>
Requirement and Part

**R1 Supporting Evidence and Documentation**

**R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

**M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

**R1 Part 1.1**

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
</table>
| 1.1   | High Impact BES Cyber Systems and their associated:  
      • PCA  
      Medium Impact BES Cyber Systems and their associated:  
      • PCA | All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. | An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP. |

The CIP v5 RSAWs are organized by Part rather than Requirement. Each part may have different Applicable Systems, and therefore different sample sets.
Registered Entity Response (Required):

**Question 1:** Do you share compliance responsibility for this Requirement with another Responsible Entity? ☐ Yes ☐ No

For example, is any BES Cyber System located at a shared facility?

If “Yes,” list the following for each asset for which compliance responsibility is shared:

1. Asset name or designation.
2. Formal agreement or other document describing the shared compliance responsibility, if any.
3. Other information regarding the shared compliance responsibility which may be useful to the audit team in determining the appropriate audit scope and approach for the asset.

Note: A separate spreadsheet or other document may be used to provide all or part of this information. If so, provide the document reference below.

Questions may be asked for circumstances beyond those covered in the Compliance Assessment Approach. In this case, any shared compliance responsibility needs to be communicated to the audit team so the proper review can be performed.
The Compliance Narrative is the place to tell the compliance monitoring team how you approach compliance with this Part. This may be the most important section of the RSAW.
Evidence Provided

Registered Entity Evidence *(Required)*:
The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Document Title</th>
<th>Revision or Version</th>
<th>Document Date</th>
<th>Relevant Page(s) or Section(s)</th>
<th>Description of Applicability of Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP_def_procV2.1.pdf</td>
<td>ESP Definition Procedure</td>
<td>2.1</td>
<td>May 7, 2015</td>
<td>4-7</td>
<td>Implemented to identify all ESPs.</td>
</tr>
</tbody>
</table>

Audit Team Evidence Reviewed *(This section to be completed by the Compliance Enforcement Authority)*:
Compliance Assessment Approach Specific to CIP-005-5, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

<table>
<thead>
<tr>
<th>Compliance Assessment Approach Specific to CIP-005-5, R1, Part 1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the Responsible Entity has documented one or more process(es) which require all applicable Cyber Assets connected to a network via a routable protocol reside within a defined ESP.</td>
</tr>
<tr>
<td>Verify each Cyber Asset of an Applicable System that is connected to a network via a routable protocol resides within a defined ESP.</td>
</tr>
<tr>
<td>For each defined ESP, verify the identification of any associated PCA.</td>
</tr>
</tbody>
</table>

Notes to Auditor:

1. This Part is applicable to all high and medium impact BES Cyber Systems for Loss of External Routable Connectivity.
2. Those Cyber Assets that are part of a high or medium impact BES Cyber System that are not connected to a network via a routable protocol need not reside within a defined ESP.
3. For Cyber Assets that are part of a high or medium impact BES Cyber System that do not reside within a defined ESP, the absence of a connection to a network via a routable protocol will be verified.
4. The reason to identify an ESP without external Routable Connectivity is to identify the PCA associated with the ESP.
5. In order to verify that each Cyber Asset residing within a defined ESP has been identified as either a BES Cyber Asset or as a PCA, it may be necessary to examine the ESP and conduct an inventory of network connections within the ESP.
6. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same defined ESP.

One or more “verify” steps
Compliance Assessment Approach Specific to CIP-005-5, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority.

Verify the Responsible Entity has documented one or more processes for authentication for all Interactive Remote Access sessions.

Verify all Interactive Remote Access sessions require multi-factor authentication as per TFE covers this circumstance.

According to this Part, verify the compensating measures have been implemented.

Auditor Notes:

Select Section

Collapse/Expand

Navigation Pane

View Menu
RSAW Compliance Assessment Approach

➢ Types of Review

• Documentation Review
  – Does the required documentation exist?
  – Does the required documentation look reasonable and complete?

• Process Evaluation
  – Does the process include the required steps?
  – Is the process adequate to ensure security?
  – Is the process adequate to ensure compliance?

• Outcome Verification
  – Has the entity performed the compliance tasks required by the Standard?
  – Has the entity adequately secured its assets as intended by the Standard?
RSAW Compliance Assessment Approach

➢ Types of Review

• Documentation Review
  – Does the required documentation exist?
  – Does the required documentation look reasonable and complete?

• Process Evaluation
  – Does the process include the required steps?
  – Is the process adequate to ensure security?
  – Is the process adequate to ensure compliance?

• Outcome Verification
  – Has the entity performed the compliance tasks required by the Standard?
  – Has the entity adequately secured its assets as intended by the Standard?
RSAW Compliance Assessment Approach

Types of Review

- Documentation Review
  - Does the required documentation exist?
  - Does the required documentation look reasonable and complete?

- Process Evaluation
  - Does the process include the required steps?
  - Is the process adequate to ensure security?
  - Is the process adequate to ensure compliance?

- Outcome Verification
  - Has the entity performed the compliance tasks required by the Standard?
  - Has the entity adequately secured its assets as intended by the Standard?

Part of Internal Controls Evaluation
RSAW CAA Special Considerations

- **Proving a Negative**
  - Review process
  - Review implementation of process
  - Sample negative results
  - Attestation – last resort
  - Example
    - CIP-002-5.1 R1 – BES Cyber Assets

- **Implied Requirements**
  - Requirements not explicitly stated but implied by the language
  - Example
    - CIP-005-5 R1 Part 1.1 – Identification of PCA
Compliance Assessment Approach Specific to CIP-005-5, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

<table>
<thead>
<tr>
<th>Verify the Responsible Entity has documented one or more process(es) which require all applicable Cyber Assets connected to a network via a routable protocol to reside within a defined ESP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify each Cyber Asset of an Applicable System that is connected to a network via a routable protocol resides within a defined ESP.</td>
</tr>
<tr>
<td>For each defined ESP, verify the identification of any associated PCA.</td>
</tr>
</tbody>
</table>

➢ Process Evaluation
  • Verify a process exists for the identification of ESPs. Verify the process requires that all applicable Cyber Assets reside within an ESP.

➢ Outcome Verification/Show a Negative
  • From the inventory of Cyber Assets associated with one or more high or medium impact BES Cyber Systems, identify all Cyber Assets connected to a network with a routable protocol. Verify each of the Cyber Assets is protected by a defined ESP, and that no BES Cyber Assets networked via a routable protocol have been missed.

➢ Outcome Verification/Implied Requirement
  • After the ESP is defined, verify the “implied” requirement of identifying any PCA within the ESP has been completed.
Process Evaluation

- Does the Cyber Security Incident response plan contain the required steps?

- A process evaluation is needed since this Requirement does not call for implementation of the plan. That happens in R2.
### Compliance Assessment Approach Specific to CIP-004-6, R3, Part 3.1

**This section to be completed by the Compliance Enforcement Authority**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Evaluation</td>
<td>• Does the process contain the required steps?</td>
</tr>
<tr>
<td>Documentation Review</td>
<td>• Review documentation that the process was implemented. This may include a review of a redacted personnel risk assessment, or other documentation may be reviewed to verify compliance. This is due to the extremely sensitive nature of the compliance evidence.</td>
</tr>
</tbody>
</table>

Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that include a process to confirm identity.

Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.
### Compliance Assessment Approach Specific to CIP-007-6, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

<table>
<thead>
<tr>
<th>Verify the Responsible Entity has documented one or more processes, for applicable patches identified in Part 2.2, to take one of the following actions within 35 calendar days of the evaluation completion:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Apply the applicable patches;</td>
</tr>
<tr>
<td>• Create a dated mitigation plan; or</td>
</tr>
<tr>
<td>• Revise an existing mitigation plan.</td>
</tr>
</tbody>
</table>

| Verify the Responsible Entity has documented one or more processes for its mitigation plans that requires the inclusion of planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations. |

<table>
<thead>
<tr>
<th>For each applicable security patch, verify that one of the following actions was taken within 35 calendar days of the completion of the evaluation for applicability:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The patch was applied to all devices for which it is applicable;</td>
</tr>
<tr>
<td>• A mitigation plan was created; or</td>
</tr>
<tr>
<td>• A mitigation plan was revised.</td>
</tr>
</tbody>
</table>

| In the case where a mitigation plan was created or revised, verify the mitigation plan includes planned actions to mitigate the vulnerabilities addressed by each security patch, and that the mitigation plan includes a timeframe for completion. |

**Note to Auditor:**

Entities may choose to use a single mitigation plan for multiple patches. In this case, the mitigation plan must have planned actions to mitigate the vulnerabilities addressed by each security patch.
Process Evaluation

- Does the patch management process have the required steps?
- Do the required steps include the creation of mitigation plans with the required elements?
For each applicable security patch, verify that one of the following actions was taken within 35 calendar days of the completion of the evaluation for applicability:

- The patch was applied to all devices for which it is applicable;
- A mitigation plan was created; or
- A mitigation plan was revised.

In the case where a mitigation plan was created or revised, verify the mitigation plan includes planned actions to mitigate the vulnerabilities addressed by each security patch, and that the mitigation plan includes a timeframe for completion.

Note to Auditor:
Entities may choose to use a single mitigation plan for multiple patches. In this case, the mitigation plan must have planned actions to mitigate the vulnerabilities addressed by each security patch.

➢ Outcome Verification
  - Did the patch management process result in systems that are patched as required, or are unpatched systems part of a mitigation plan?

➢ Documentation Review
  - Did any mitigation plan include the required elements?
Tips for Using the RSAW$s$

- Avoid unnecessary redundancy – use references where possible; otherwise copy and paste. If a process applies to an entire Requirement, describe it in one Part and make reference to it elsewhere.

- The Compliance Narrative is your best opportunity to tell an audit team how you meet compliance.

- Pay attention to any “Notes to Auditor.” They’re meant for you, too.
EVIDENCE
Evidence Overview

Initial Evidence Request

Sampling Populations (minimal detail)
- BES Cyber Systems
- Cyber Assets
- Assets
- Personnel
- CIP Exceptional Circumstances
- Technical Feasibility Exceptions

Compliance Documents
- Policy
- Process
- Plan
- Program
- Procedure

Initial Sampling

Multiple Sample Sets
Sample set appropriate to Requirement and/or Part
Evidence specific to each Requirement
Additional sampling may be advisable
Evidence Types

➢ Compliance Documents
  • Policy
  • Process
  • Plan
  • Program
  • Procedure

➢ Evidence of Compliance Pertaining to:
  • Cyber Assets
  • BES Cyber Systems
  • Assets
  • Personnel
  • CIP Exceptional Circumstances
  • Technical Feasibility Exceptions
Sampling Overview

Sampling Guideline

- Current Guideline updated September 4, 2013
- References RAT-STATS
- New revision in progress
  - Will be an Addendum to the ERO Compliance Auditor Handbook
- CIP-specific Addendum is planned by the end of 2015

Sampling Process (greatly simplified)

- Determine sample size
- Choose sampling method
- Select sample
Sample Sets

- Expect to see different sample sets, such as:
  - High impact BES Cyber Systems
  - Cyber Assets of an Applicable System
  - Electronic Security Perimeters
  - Cyber Assets within a specific set of ESPs

As the sampling methodologies take shape, the development team will attempt to minimize redundancy, but this will be difficult due to the divergent applicability of the Parts of some Requirements. The following slide demonstrates some of the complexity.
As you can see, the number of applicable parts varies widely depending on the type of Cyber Asset under consideration. This will make the sampling process far more complex than that of CIPv3.
IRA and ICE

- **IRA – Inherent Risk Assessment**
  - Based on registrations, entity size, compliance history, etc.
  - Determines initial scope of compliance assessment
  - Provides risk levels to other processes

- **ICE – Internal Controls Evaluation**
  - Based on voluntary review of internal controls
  - Can affect:
  - Scope of compliance assessment
  - Depth of compliance assessment (e.g., sample size)
  - Frequency of audits
Questions & Answers

Forward Together • ReliabilityFirst