Compliance Webinar

Fall 2010

December 14 & 15

Standard Review - CIP-009
(Recovery Plans for Critical Cyber Assets)

Shon Austin, Senior Compliance Specialist
CIP-009 Purpose

CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.
CIP-009 Requirements

- R1. Recovery Plan(s)
- R2. Exercising the Recovery Plan(s)
- R3. Change Control (Updates)
- R4. Backup and Restore
- R5. Testing Backup Media
CIP-009 Violations in the SPP RE as of November 30, 2010

<table>
<thead>
<tr>
<th>CIP-009-1 by Requirement</th>
<th>Number of Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 1 – Recovery Plan(s)</td>
<td>7</td>
</tr>
<tr>
<td>Requirement 2 - Exercises</td>
<td>10</td>
</tr>
<tr>
<td>Requirement 3 – Change Control</td>
<td>0</td>
</tr>
<tr>
<td>Requirement 4 – Backup and Restore</td>
<td>1</td>
</tr>
<tr>
<td>Requirement 5 - Testing Backup Media</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total Violations</strong></td>
<td><strong>20</strong></td>
</tr>
</tbody>
</table>

10 entities out of 17 spot checked entities
CIP-009 R1 - Recovery Plans

Recovery Plans — The Responsible Entity shall **create** and **annually review** recovery plan(s) for **Critical Cyber Assets**. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the **required actions** in response to events or conditions of **varying duration and severity** that would activate the recovery plan(s).

R1.2. Define the **roles** and **responsibilities** of responders.
Key Reasons for Non-Compliance

- The Responsible Entity has not created a recovery plan for CCAs
- The Responsible Entity has created but not annually reviewed recovery plan(s) for CCAs
- The Recovery Plan(s) did not specify any required actions in response to events or conditions of varying duration and/or severity that would activate the recovery plan(s).
- The Recovery Plan(s) did not define the roles and responsibilities of responders
Process Enhancement for CIP-009 R1

• The Responsible Entity shall create and annually review recovery plan(s) for CCAs.

• The Recovery Plan(s) must:
  
  A. identify actions resulting from incidents of “varying duration and severity”.

  B. define the “roles and responsibilities” of responders to the aforementioned incidents.
CIP-009 R2 - Exercises

• Exercises — The recovery plan(s) shall be exercised at least **annually**. An exercise of the recovery plan(s) can range from a **paper drill**, to a **full operational exercise**, to **recovery from an actual incident**.
Key Reasons for Non-Compliance

• The Responsible Entity's recovery plan(s) have not been exercised annually.

• The Responsible Entity failed to follow/adhere or provide evidence that its recovery plan was exercised or a recovery from an actual incident that invoked the recovery plan was performed.

• The Responsible Entity performed a recovery exercise but failed to recover a Critical Cyber Asset.
Process Enhancement for CIP-009 R2

- The Responsible Entity's recovery plan(s) must be exercised annually.

- The Responsible Entity must follow and document evidence that its recovery plan was exercised or a recovery from an actual incident that invoked the recovery plan was performed.

- The Responsible Entity must recover a CCA.
CIP-009 R3 - Change Control

- Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.
Key Reasons for Non-Compliance

- The Responsible Entity failed to update or provide evidence that recovery plan(s) have been updated to reflect changes.
- The Responsible Entity did not provide evidence of communication to the personnel responsible for the activation and implementation of the recovery plan(s) within 30 calendar days of the change.
Process Enhancement for CIP-009 R3

- The Responsible Entity's recovery plan(s) must be updated to reflect any changes or lessons learned.
- The Responsible Entity’s Recovery Plan(s) must communicate the change within 30 calendar days to the personnel responsible for the activation and implementation of the Recovery Plan(s).
CIP-009 R4 - Backup and Restore

• Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.
Key Reasons for Non-Compliance

- The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
Process Enhancement for R4

- The Responsible Entity's recovery plan(s) must include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009 R5 - Testing Backup Media

- Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.
Key Reasons for Non-Compliance

- The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.
Process Enhancement for R5

- The Responsible Entity's information essential to recovery that is stored on backup media must be tested annually to ensure that the information is available.

- An entity should ask itself “How do we know we have all essential information to recover our system stored on a backup media”.
In Summary

- R1. Recovery Plan(s)
- R2. Exercising the Recovery Plan(s)
- R3. Change Control (Updates)
- R4. Backup and Restore
- R5. Testing Backup Media
CIP Compliance Monitoring Team

- **Kevin B. Perry**
  Director, CIP
  (501) 614-3251
  kperry@spp.org

- **Steve Applegate**
  Lead Compliance Specialist
  (501) 688-1633
  sapplegate@spp.org

- **Shon Austin**
  Sr. Compliance Specialist
  (501) 614-3273
  saustin@spp.org

- **Leesa Oakes**
  Compliance Specialist II
  (501) 614-3274
  loakes@spp.org
Resources

- CDW Business Continuity: (http://www.cdw.com/content/solutions/business-continuity/)
Questions