Loss of Control
Center Functionality:
EOP-008-1, CIP-008-3,
CIP-009-3
September 30, 2014

James Williams
Lead Compliance Specialist
jwilliams.re@spp.org
501.614.3261

Jeremy Withers
Senior Compliance Specialist - CIP
jwithers.re@spp.org
501.688.1676

Southwest Power Pool
Regional Entity
Related Standards

• **EOP-008-1**: Ensure continued reliable operation of the Bulk Electric System (BES) in the event that a control center becomes inoperable.

• **CIP-008-3**: Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

• **CIP-009-3**: Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established disaster recovery techniques and practices.
EMS Outage Scenario

• It is 16:00 on August 21 and the forecasted temperatures are expected to reach 98 degrees

• Load projection is at peak levels

• The NERC Certified Senior System Operator noticed he no longer had visibility of the Transmission System and he cannot use the transmission desk EMS console to adjust flows as necessary
Scenario

• Operator assessed the situation
  – Primary control center EMS has completely failed and it would not fail over to standby system

• Operators were trained on the evacuation plan, which covered many scenarios including:
  – Fire
  – Tornado
  – Loss of EMS
  – Loss of communication

• Assumed EMS at back-up control center is functional

• Operators decided to evacuate primary and relocate to back-up (EOP-008-1 R1.4)
Scenario

• By following the Evacuation Plan
  – Notified Reliability Coordinator and neighboring TOPs (R1.6.1) to monitor the ties (R1.6.2)
  – Notified management and other support personnel (R1.6.3)
  – Took the Evac-Bag, which included:
    ▪ Cell phone
    ▪ Evacuation and start-up checklist
    ▪ Operating Plan
Scenario

• Arrived at back-up center
  – Took longer than during drills (drills were not during the rush hour)

• Started systems by using the start-up checklist
  – Phone systems, EMS and corporate system tools

• Functional within a 2-hour window (R1.5)

• Contacted the RC and neighboring TOPs that the back-up is functional
  – Operator confirmed tie-line reading with the neighboring TOPs

• Contacted IT department to investigate EMS outage of primary control center
What issues could you encounter in a scenario like this?

- **Uncertainty of the back-up EMS**
  - Was it having the same issue as the primary?
  - Waiting on IT to make the decision to evacuate

- **Operating Plan and training**
  - Did the operating plan cover the scenario?
  - Were the operators trained on a similar scenario?
  - During the training, were operators put under stress, as in a real event?
  - Is your training and plan too rigid? Is it adaptable to circumstances?
Do not forget Event forms

- EOP-004-2 R1 – report in accordance to EOP-004-2 Attachment 1
- EOP-004-2 R2 - within 24 hours of recognition of meeting an event type
  - Event Type: Unplanned BES control center evacuation
  - Responsibility: RC, BA, TOP
  - Threshold for Reporting: Unplanned evacuation from BES control center facility for 30 continuous minutes or more.
  - Event Type: Complete loss of monitoring capability
  - Responsibility: RC, BA, TOP
  - Threshold for Reporting: Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more sure that analysis capability is rendered inoperable.
Requirements we commonly see issues with

- **R1** requires plan for moving from primary to back-up
  - Are personnel identified in the Operating Plan involved in training?
  - Drill times aren’t being documented
- **R2** Operating Plan copies at primary and back-up
- **R3** and **R4** Does back-up center provide the same functionality as your primary?
- **R5** Annual review and approve the Operating Plan
  - In plan’s revision history, document when annual review was conducted and who approved it
Requirements we commonly see issues with

• **R6** Primary and back-up should not depend on each other

• **R7** Conduct annual test of Operating Plan
  – **R7.1** Transition time from primary to back-up functionality
  – **R7.2** Back-up needs to be fully functioning for a minimum of two continuous hours
EOP-008-1 Best Practices*

• Hold unannounced drills
  – Are drills “real life”?  
  – Do people have a sense of urgency during the drills?

• Use different scenarios
  – Ensure Operating Plan works for different scenarios, not just one such as fire

• All personnel identified in the Operating Plan should take part in the drills

• Document in the Operating Plan revision history that it was annually reviewed and approved

* These best practices are not required
Internal Controls

• **Preventive:**
  – Having a robust Operating Plan that is reviewed annually
  – Annually training staff on Operating Plan, using “real life” situations
  – Testing back-up capabilities

• **Detective:**
  – Alarms that notify Operators of issues
    ▪ Fire, EMS alarms

• **Corrective:**
  – Revising Operating Plan based on issues found during review and training **or** actual event
    ▪ Root cause analysis of actual events
  – Retraining personnel on any Operating Plan revisions
IT’s Response to EMS Outage Scenario

• Received phone call from Operations regarding evacuation
• Arrived with hard copy of Cyber Security Incident Response plan (CSIRP)
• Rebooted SCADA server and kept getting “Blue Screen of Death”
• Noticed open ports not on the baseline (port 25, port 69, port 80, etc.)
• Declared a reportable Cyber Security Incident due to the large number of open ports and anti-virus scan results (CIP-008-3 R1.1)
IT’s Response to EMS Outage Scenario

• Notified all personnel listed on the CSIRP call sheet (CIP-008-3 R1.2)

• Each member arrived with their assigned CSIRP hard copy and proceeded with their assigned role (CIP-008-3 R1.2)

• Ensured containment of the malware by disconnecting asset from network (CIP-008-3 R1.2)

• CSIRP team lead notified Electricity Sector Information Sharing and Analysis Center (ES-ISAC) via telephone (CIP-008-3 R1.3)
IT’s Response to EMS Outage Scenario

- Scanned all assets in the Electronic Security Perimeter (CIP-009-3 R1)
- Found primary and standby SCADA servers had been compromised with malware (CIP-009-3 R1.1)
- IT lead proceeded to recover the asset per the recovery plan (CIP-009-3 R1.2)
- Backup media retrieved and installed (CIP-009-3 R4)
- Post-installation scans performed
- Verified EMS was properly functioning
Lessons Learned

• Added “prosecution” slide to annual cyber security training
• Create an e-mail distribution group for Cyber Security Incidents
  – Helpful with documentation retention
• Include hardware and SCADA vendor contact numbers in recovery plan
• Specify minimum relevant documentation to retain in CSIRP (CIP-008-3 R2)
  – E-mails
  – Logs (system and phone)
What problems could IT encounter in such as a scenario?

• IT pulled outdated hard copy of plan from shelf
• Not having ES-ISAC contact information listed in plan
• Reliance on a single person for a response task
• Not recognizing situation and responding appropriately
• Not completing after-action review
• Not updating plan with lessons learned
Common issues we see with CIP-008/009

- **CIP-008-3 R1.6**: requires annual testing of plan
  - Failure to document actual testing of the plan
    - Real incident can serve as a test, but you must document it
  - Execution of plan did not generally follow the plan’s steps
  - Test scenario did not include a Critical Cyber Asset
  - Did not have appropriate people at test
Common issues we see with CIP-008/009

- **CIP 009 R2**: requires annual testing of plan
  - Not following recovery plan steps
  - Scope does not include all required assets
    - CIP-005-3 R1.5
    - CIP-006-3 R2.2
    - These assets are now included in the Applicability column for each cyber security requirement in CIP version 5
  - Not verifying that back-up media is useable
CIP-008/009 Best Practices*

- Bare metal restore in a test environment
- Catalog back-up media
- Have multiple rotating back-up sets
- Have procedures and configuration documentation in hard copy and included in recovery plans
- Have hard copies of plans (CSIRP and recovery)
- Understand current threat landscape
- Unscheduled response and recovery plan exercises
- Test different scenarios that would invoke recovery and response plans

* Best practices are not required
Internal Controls

- Response plans and recovery plans are security controls focused on availability
Internal Controls Used in Scenario

- Having back-ups: Preventive
- Performing training: Preventive
- Performing port scans: Detective
- Performing anti-virus scans: Detective
- Reviewing Logs: Detective
- Recovering assets per plan: Corrective
- Lessons learned: Corrective
V3-V5 REFERENCE SLIDES
CIP-008-3 vs. CIP-008-5: What’s new?

• CIP-008-3 R1
  – (CIP-008-5 R1 Part 1.1) Wording changes:
    ▪ “identify” instead of “Characterize”
    ▪ “respond to” instead of “Response actions”

• CIP-008-3 R1.1
  – (CIP-008-5 R1 Part 1.2): Reportable Cyber Security Incident - A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity
  – (CIP-008-5 R1 Part 1.2): Report to the ES-ISAC within 1 hour from the determination of a Reportable Cyber Security Incident
CIP-008-3 vs. CIP-008-5: What’s new?

• CIP-008-3 R1.2
  – (CIP-008-5 R1 Part 1.3) Wording changes:
    ▪ “incident response groups or individuals” instead of “incident response teams”

• CIP-008-3 R1.3 (Deleted)

• CIP-008-3 R1.4 & CIP-008-3 R1.5
  – (CIP-008-5 R3 Part 3.1):
    ▪ Changes that require an update to the Response Plan are clear
    ▪ Timing requirement: 90 calendar days following testing or an actual Reportable Cyber Security Incident response
CIP-008-3 vs. CIP-008-5: What’s new?

- CIP-008-3 R1.4 & CIP-008-3 R1.5 (cont.)
  - (CIP-008-5 R3 Part 3.1.1):
    - Document any lessons learned or document the absence of any lessons learned (NEW)
  - (CIP-008-5 R3 Part 3.1.2):
    - Update response plan based on documented lessons learned
  - (CIP-008-5 R3 Part 3.1.3):
    - Communication of response plan changes to each person or group with a defined role in the response plan based on lessons learned (NEW)
CIP-008-3 vs. CIP-008-5: What’s new?

- **CIP-008-3 R1.6**
  - (CIP-008-5 R2 Part 2.1):
    - Response plan must be tested at least once every 15 calendar months
  - (CIP-008-5 R2 Part 2.2):
    - Deviations from the response plan (in response to the incident or an exercise of the plan) must be documented

- **CIP-008-3 R2**
  - (CIP-008-5 R2 Part 2.3):
    - Retention period of 3 calendar years addressed in the Compliance section
CIP-008-3 vs. CIP-008-5: What’s new?

• Other notable changes

• CIP-008-5 R3 Part 3.2:
  – No later than 60 calendar days after a change to the roles and responsibilities, Cyber Security Incident groups or individuals, or technology that would impact the ability to execute the plan:
    ▪ Response plan must be updated
    ▪ Each person or group with a defined role in the response plan must be notified of the updates
CIP-009-3 vs. CIP-009-5: What’s new?

• CIP-009-3 R1
  – (CIP-009-5 R3 Part 3.1):
    ▪ Added requirement for documentation of any identified deficiencies or lessons learned
  – (CIP-009-5 R3 Part 3.2):
    ▪ Added the requirement to additionally review plans after technology changes
CIP-009-3 vs. CIP-009-5: What’s new?

• CIP-009-3 R1 (cont.)
  – (CIP-009-5 R3 Part 3.1.1):
    ▪ Added requirement parts to document any lessons learned
  – (CIP-009-5 R3 Part 3.1.2):
    ▪ Update recovery plan based on documented lessons learned
  – (CIP-009-5 R3 Part 3.1.3):
    ▪ Notify each person or group of any updates to the recovery plan
CIP-009-3 vs. CIP-009-5: What’s new?

• CIP-009-3 R1.1 & CIP-009-3 R1.2 (no significant changes)

• CIP-009-3 R2
  – (CIP-009-5 R2 Part 2.1):
    ▪ Recovery plan must be tested at least once every 15 calendar months

• CIP-009-3 R3
  – (CIP-009-5 R3 Part 3.2):
    ▪ Time frame for updates is no later than 60 calendar days following a change
CIP-009-3 vs. CIP-009-5: What’s new?

- CIP-009-3 R4 (no significant changes)
- CIP-009-3 R5
  - (CIP-009-5 R2 Part 2.2):
    - Information used to recover BES Cyber System functionality must be tested at least once every 15 calendar months
CIP-009-3 vs. CIP-009-5: What’s new?

- Other notable changes
  - (CIP-009-5 R1 Part 1.4)
    - One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.
  - (CIP-009-5 R1 Part 1.5)
    - Process to preserve data for analysis
CIP-009-3 vs. CIP-009-5: What’s new?

• Other notable changes
  – (CIP-009-5 R2 Part 2.3)
    ▪ Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.
  – (CIP-009-5 R3 Part 3.1 & Part 3.2)
    ▪ Communicate recovery plan updates
Additional Resources

- NIST SP 800-53
- NIST SP 800-61
- NIST SP 800-34
Summary

• EMS failures are a common cause of reportable events
• It’s very important to train on different scenarios and involve all identified personnel
• Training should mimic a real-life situation as much as possible
• Team cross-training is important
• Plans should be updated based on training and after-action lessons learned