CIP Standards
Violation Analysis

Kevin B. Perry
kperry.re@spp.org · 501.614.3251

July 24, 2013
Total CIP-002 – CIP-009 Violations

By Standard

- CIP-007: 30%
- CIP-006: 12%
- CIP-005: 16%
- CIP-004: 15%
- CIP-003: 10%
- CIP-002: 8%
- CIP-009: 6%
- CIP-008: 3%

SPP RE Region
359 CIP Violations 2008-2012

By Year

- 2008: 0
- 2009: 20
- 2010: 40
- 2011: 80
- 2012: 140

Number of Violations
Self-Reported versus RE Discovered Violations

- Self ID: 61%
- SPP RE ID: 39%

### Bar Graph 1
- Years: 2008 to 2012
- Data: SPP RE ID and Self ID

### Bar Graph 2
- Years: 2008 to 2012
- Data: SPP RE ID and Self ID

### Pie Chart
- 61% Self ID
- 39% SPP RE ID
Violations Annual Trend By Standard

CIP-009
CIP-008
CIP-007
CIP-006
CIP-005
CIP-004
CIP-003
CIP-002

2008
2009
2010
2011
2012
CIP-007 / R5: Account Management

- Entity staff do not verify vendor support engineer is on authorized access list before granting access.
- User access is not logged – only login failures are recorded.
- User account created without authorization.
- Shared user account not secured upon voluntary termination of individual with access.
- Local password had not been changed in 1,706 days.
- Shared user account password not changed annually.
- Users with access to shared account not documented.
CIP-007 / R5: Account Management

• Factory default account password not changed before placing Cyber Asset into service.

• Use of the shared user account is logged, but not the identity of the individual using the shared account.

• Number of local and domain user passwords not changed annually.

• Not all passwords meet complexity requirement.

• Required technical and procedural controls not documented nor implemented.

• Access not granted on need-to-know basis.
CIP-006 / R1: Physical Security Plan

- Visitor to PSP not provided continuous escort.
- Visitor escort (security guard) did not have authorized, unescorted access into PSP.
- “Lost” employee tail-gated into PSP without being detected by distracted employee with authorized, unescorted access.
- Not all Cyber Assets within an ESP reside within a PSP.
- Not all physical access control systems afforded protections of CIP standard requirements.
- Data cable between two discrete PSPs not protected.
CIP-006 / R1: Physical Security Plan

- PSP not enclosed within a full six-wall boundary and no alternative protections implemented.
- Security Plan not approved by the CIP Senior Manager.
- Security Plan does not address all required elements.
- Physical access granted by personnel not authorized to grant such access.
- Physical Security Perimeter and controls not documented.
- Visitor access not logged (incomplete log entries).
CIP-005 / R2: Electronic Access Controls

• Required organizational processes and technical and procedural controls not documented nor implemented.

• Required ports and services not documented.

• Unable to demonstrate that only ports and services required for operations and monitoring of Cyber Assets have been enabled.

• Excess firewall rule permissions configured.

• Firewall access control lists defined but not applied to an interface.
CIP-005 / R2: Electronic Access Controls

• Electronic access not reviewed quarterly.
• External interactive access not strongly authenticated at the ESP access point.
• Firewall rules remain configured for Cyber Assets previously removed from service.
• No access controls configured on circuit between two Electronic Access Perimeters.
• Acceptable use banner not displayed until after successful user log-in.
CIP-005 / R1: Electronic Security Perimeter

• Not all electronic access control and monitoring systems afforded protections of CIP standard requirements.

• Security event logs not retained for at least 90 days.

• Not every Critical Cyber Asset resides within an ESP.

• Not all Cyber Assets comprising the EACMS reside within a PSP.

• Not all electronic access points have been identified and documented.
CIP-004 / R4 - Access

- Access lists incomplete or inaccurately updated.
- Not all electronic and physical access documented.
- Specific access rights not documented.
- Access not removed for terminated personnel within the required timeframe.
- Unable to demonstrate access lists were reviewed quarterly.
- Quarterly access review did not include access rights.
- Vendor personnel access not documented or reviewed.
CIP-007 / R3: Security Patch Management

- Assessment of available security patches not completed within 30 days.
- Third-party security patches not assessed for applicability.
- Security patches not assessed for all in-scope Cyber Assets.
- Documentation of security patch assessment not retained.
- Security patch not installed and no compensating measures documented and/or implemented.
CIP-007 / R1: Test Procedures

- Application functionality is tested, but there is no testing for adverse impact to security controls.
- Not all in-scope Cyber Assets subjected to security controls testing as part of security updates.
- Cyber security controls testing not performed for installed updates or for new Cyber Assets.
- Transient laptop connected into ESP without performing cyber security controls testing.
- Test procedures not documented or maintained.
- Test results not documented or not retained.
CIP-007 / R6: Security Status Monitoring

• Security event logs not reviewed.
• Security events not monitored on one or more in-scope Cyber Assets.
• Automated alerting process is improperly configured for certain Cyber Assets.
• Security event logs not retained for minimum of 90 days.
• Cyber Asset not able to log and no TFE requested.
CIP-007 / R4: Malicious Software Prevention

• Anti-virus management console not monitored by staff for virus alerts.

• Anti-virus signature files not tested before update applied.

• Anti-virus/anti-malware not implemented and no TFE requested.

• Anti-virus software installed but found not operational on Cyber Asset.
CIP-005 / R4: Cyber Vulnerability Assessment

• No documented Cyber Vulnerability Assessment process.
• No evidence that enabled ports and services are reviewed.
• Firewall rules are not reviewed.
• Insufficient and ineffective ESP access point identification process.
• Undocumented ESP access point not found by CVA.
• Community strings not reviewed.
CIP-006 / R2: Protection of PACS

- Gaps in retained logs.
- Logs retained but not reviewed for security events.
- Unmonitored physical access point.
- Not all physical access control systems afforded protections of CIP standard requirements.
Mitigations and Assistance

• SPP RE Offers:
  – Annual CIP Compliance Workshop
  – Webinars
  – Video Presentations
  – “Ask the RE” Outreach

• SPP, Inc. Offers:
  – Pre-audit Evidence Reviews
  – Compliance Forum
  – Critical Infrastructure Protection Working Group

• NERC Offers:
  – Compliance Application Reports (for now)
  – Electricity Sector Information Sharing and Analysis Center
SPP RE Training Videos:
vimeopro.com/sppre/basics

- Audits: Top 10 Ways to Prepare
- CIP Audit: What to Expect
- CIP-005: Electronic Security Perimeter
- CIP-005-3 R3
- CIP-006: Physical Security
- CIP-007 Compliance
- CIP-007: R1 System Configuration
- CIP-007 R3 and R4
- Compliance Education at My Company
- Internal Compliance Programs Q&A
- Event Analysis-Entity Perspective
- Evidence Submission
- Firewalls: 13 Ways to Break Through
- Hashing: How To
- Human Performance - Entity Perspective
- Human Performance - NERC
- Mitigation Plans: Milestones, Completion, and Evidence
- Mock 693 Audit
- Self-Reporting: When and How
- TFE Expectations and Issues
- Training Employees on Compliance
ADDITIONAL INFORMATION
Violations Annual Trend By Requirement

2008
2009
2010
2011
2012

C9/R5
C9/R4
C9/R3
C9/R2
C9/R1
C8/R2
C8/R1
C7/R9
C7/R8
C7/R7
C7/R6
C7/R5
C7/R4
C7/R3
C7/R2
C7/R1
C6/R8
C6/R7
C6/R6
C6/R5
C6/R4
C6/R3
C6/R2
C6/R1
C5/R5
C5/R4
C5/R3
C5/R2
C5/R1
C4/R4
C4/R3
C4/R2
C4/R1
C3/R6
C3/R5
C3/R4
C3/R3
C3/R2
C3/R1
C2/R4
C2/R3
C2/R2
C2/R1
Resource Links

• SPP RE Resources
  – Workshops, Webinars, Videos
    http://www.spp.org/section.asp?pageID=92

• SPP, Inc. Resources
  – RTO Compliance Department Services
    http://www.spp.org/section.asp?pageid=159

• NERC Resources
  – Compliance Application Reports
  – Electricity Sector Information Sharing and Analysis Center
    http://www.esisac.com/SitePages/Home.aspx
SPP RE Contact Information

- Kevin B. Perry
  Director, Critical Infrastructure Protection
  kperry.re@spp.org
  (501) 614-3251

- Shon Austin
  Lead Compliance Specialist – CIP
  saustin.re@spp.org
  (501) 614-3273

- Steven Keller
  Senior Compliance Specialist – CIP
  skeller.re@spp.org
  (501) 688-1633

- Leesa Oakes
  Compliance Specialist II – CIP
  Loakes.re@spp.org
  (501) 614-3274

- Jeremy Withers
  Compliance Specialist II – CIP
  jwithers.re@spp.org
  (501) 688-1676