



**Compliance Analysis Report
Critical Infrastructure Protection Standards
CIP-002 through CIP-009**

**By: Ron Ciesiel
Executive Director of Compliance
Southwest Power Pool Regional Entity**

Prepared for April 26, 2010 SPP RE Trustee Meeting



SPP RE

CIP-002 through CIP-009

Violation Statistics

Year Reported and/or Discovered	Total Number of Enforceable Violations		Number of CIP-002 through CIP-009 Violations		Percent of CIP-002 through CIP-009 Violations*	
	All		All		All	
	SPP RE	Regions	SPP RE	Regions	SPP RE	Regions
2008	16	1025	4	86	25%	8%
2009	128	1197	49	303	38%	25%
2010	64	292	36	<u>149</u>	56%	51%
Total	208	2514	89	538	43%	21%

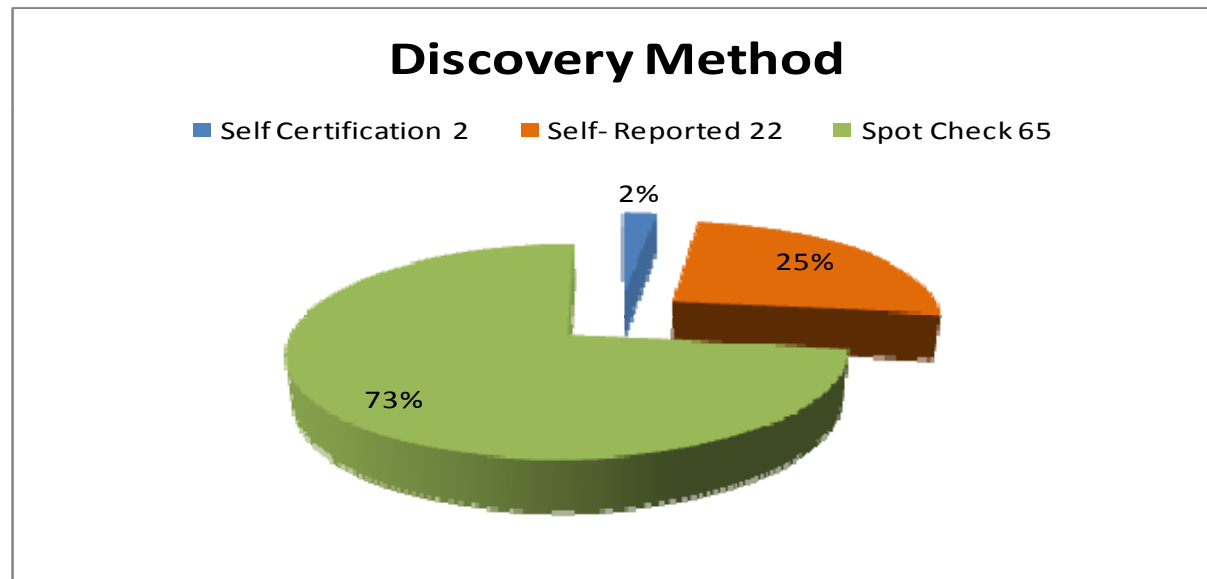
Notes:

¹ CIP-002 through CIP-009 Standards became enforceable July 1, 2008

² Number of Violations through April 1, 2010



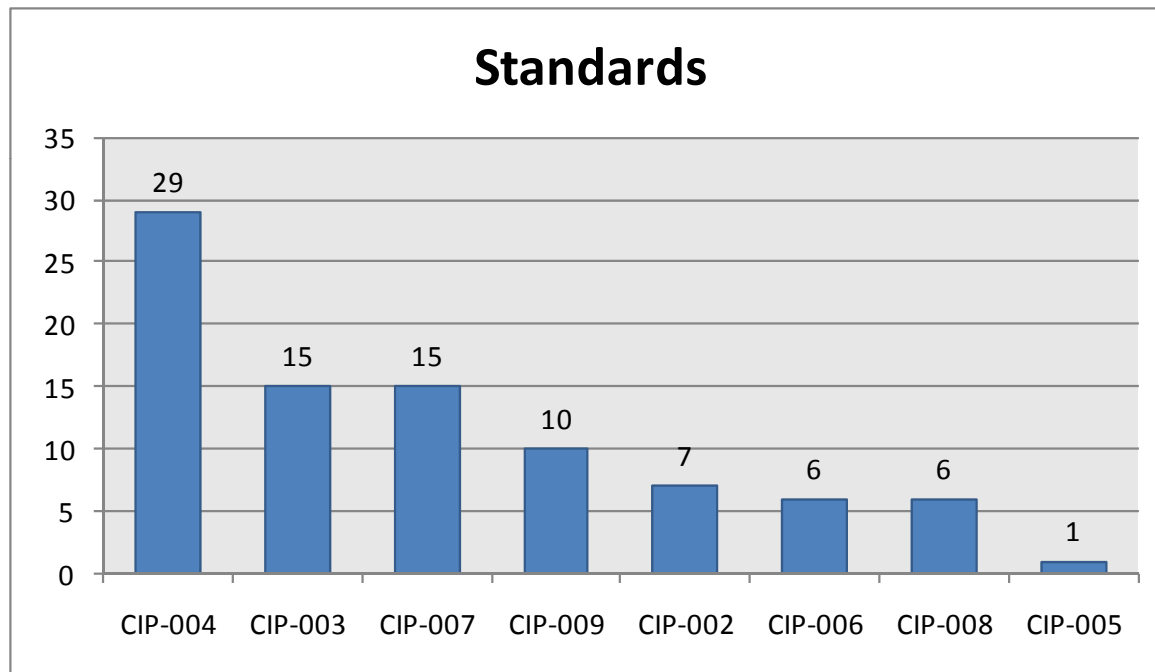
SPP RE CIP-002 through CIP-009 Violation Statistics



Number of CIP 2 through CIP 9 violations reported to and/or discovered by SPP RE through April 1, 2010



SPP RE CIP-002 through CIP-009 Violation Statistics



Number of CIP 2 through CIP 9 violations reported to and/or discovered by SPP RE through April 1, 2010



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-004: Cyber Security – Personnel & Training

- **Purpose:** Requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness
- **Common Reasons for non-compliance finding:** See Compliance Analysis Reports published by NERC and Regional Entities, December 9, 2009 (http://www.nerc.com/files/CIP-004_Combined_FINAL.pdf)
 - Training program does not include all of the required elements.
 - Not all personnel with access trained.
 - PRA not performed for all personnel with access.
 - Access list does not include specific access rights.
 - Quarterly access review does not check all personnel with access.
 - Quarterly access review does not include specific access rights.



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-003: Cyber Security — Security Management Controls

- **Purpose:** Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets
- **Common Reasons for non-compliance finding:**
 - Cyber Security Policy failed to address all of the requirements of CIP-002 through CIP-009 (R1.1)
 - Entity failed to assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, CIP-002 through CIP-009 (R2)



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-007: Cyber Security — Systems Security Management

- **Purpose:** Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s) (ESPs)
- **Common Reasons for non-compliance finding:**
 - Entity failed ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls, i.e., the entity tested the functionality of the application, but failed to test the functionality of the security controls, verified that update/patch works properly, but failed to verify the security controls have not been jeopardized (R1)
(In the context of this standard, Cyber Assets such as laptop computers that are moved into and out of the Electronic Security Perimeter must be treated as “new” Cyber Assets and be subjected to the security controls testing prescribed by the standard when connecting inside the ESP.)



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-009: Cyber Security — Recovery Plans for Critical Cyber Assets

- **Purpose:** 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.
- **Common Reasons for non-compliance finding:**
 - Entity's Recovery Plans for Critical Cyber Assets failed to include specific recovery plans for Critical Cyber Assets, i.e., the recovery plan did not include a recovery phase to reconstitute affected facilities or assets after a disaster (R1.1)
 - Entity's Recovery Plans for Critical Cyber Assets failed to clearly define roles and responsibilities (R1.2)
 - Entity failed to provide documentation demonstrating that its recovery plans have been exercised/tested at least annually. The exercise must involve Critical Cyber Assets in the exercise scenario and demonstrate the recovery plans for those Cyber Assets were followed. (R2)



SPP RE CIP-002 through CIP-009 Compliance Analysis

CIP-002: Cyber Security — Critical Cyber Asset Identification

- **Purpose:** Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System (Critical Assets are to be identified through the application of a risk-based assessment)
- **Common Reasons for non-compliance finding:** See SPP RE Assessment Monitoring and Implementation of Reliability Standard CIP-002-1, January 18, 2010 ([http://www.spp.org/publications/CIP-002-1\(R1\)-Analysis.pdf](http://www.spp.org/publications/CIP-002-1(R1)-Analysis.pdf) and CIP-002 Spot Check Results and Whitepaper, January 25, 2010 (<http://www.spp.org/publications/1.25.10%20RE%20Trustee%20Meeting%20Minutes.pdf> – Attachment 5)
 - Not all Critical Assets identified through application of the methodology
 - Methodology does not include procedure
 - Methodology does not include measurable criteria.
 - Not all Critical Cyber Assets identified
 - ICCP nodes
 - Operator consoles
 - Redundant systems



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-006: Cyber Security — Physical Security of Critical Cyber Assets

- **Purpose:** Ensures the implementation of a physical security program for the protection of Critical Cyber Assets
- **Common Reasons for non-compliance finding:**
 - Entity's physical security plan failed to address one or more of the eight items referenced in Requirement 1, (R1)
(e.g., the entity's physical security plan did not include adequate processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter (R1.1))



SPP RE

CIP-002 through CIP-009

Compliance Analysis

CIP-008: Cyber Security — Incident Reporting and Response Planning

- **Purpose:** Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets
- **Most Often Reason(s) for Findings of Non-Compliance:**
 - Entity's Cyber Security Incident response plan failed to address one or more of the six items referenced in Requirement 1, (R1)

(e.g., the entity's incident response plan failed to include procedures to characterize and classify incidents as being reportable, incident handling procedures, clearly defined roles and responsibilities or instruction for reporting to ES-ISAC (R1.1, 1.2, & 1.3)



SPP RE

CIP-002 through CIP-009 Compliance Analysis

Lessons Learned

- **Treat as a Group:** CIP-002 through CIP-009 Standards should be read comprehensively as a single group of standards due to the interrelated nature of the standards .
- **Pay Attention to Detail:** Entities should be very attentive to details when addressing the CIP standards in their policies, procedures, and plans, i.e., entities should ensure that their policies, procedures, and plans address all the elements of the standards.
- **Ensure Adequate Training:** Entities should ensure responsible personnel are identified and provided adequate training regarding the entity's cyber security policies, procedures, and plans.
- **Test and Document Results:** Entities should establish and adhere to a specified testing schedule in accordance with the standard requirements. Document sufficient to demonstrate compliance should be maintained.



Questions

