



Western Electricity Coordinating Council

# *WECC CIP Compliance*

---

WECC Compliance User Group  
Harrah's Casino Resort, Reno, NV  
April 3<sup>rd</sup>, 2008

Patrick Miller CISA CISSP-ISSAP  
WECC Sr. Compliance Engineer, Cyber Security

# *WECC CIP Compliance Staff*

---

- Patrick Miller
  - CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM
  - 20+ years in IT
  - 8+ years in Energy
  - WECC Sr. Compliance Engineer, Cyber Security (read: CIP Auditor)

# *Presentation Overview*

---

- CIP Past
- CIP Present
  - Implementation Plan
  - Walkthrough of the “First 13”
- CIP Outreach
- CIP WECC Cyber Security Website
- CIP Auditor Training
- CIP RSAW
- CIP Compliance Breakdown
- CIP Future
- Compliance Tips

# *CIPS In A Nutshell...*

---

- ***Critical Infrastructure Protection Standards (CIPS) are intended to protect the following:***
  - Bulk Power System (Bulk Electric System)
  - Critical Assets
    - Control Centers, Transmission Subs, Generation Plants
  - Critical Cyber Assets
    - EMS, DCS, RTUs, IEDs, PLCs, Relays
    - Decision Support Systems
  - Critical Infrastructure Information
- Provide greater reliability through greater security and accountability

# *CIP Past*

---

- FERC SMD Appendix G
  - NERC UAS-1200
  - NERC 1300
  - NERC CIP 002-009
  - NERC CIP-001
  - FERC Order 693
  - FERC Staff Assessment
  - FERC CIPS NOPR
  - FERC Order 706
- Influential Factors
    - NE Blackout 2003
    - “Aurora”
    - SANS CIA briefing
    - News media in general

# *CIP Present*

---

- CIP-001: Sabotage Reporting
- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter(s)
- CIP-006: Physical Security of CCAs
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for CCAs
  
- FAQ and Implementation Plan

# Implementation Plan

**Table 1**  
**Compliance Schedule for Standards CIP-002-1 through CIP-009-1**  
**Balancing Authorities and Transmission Operators Required to Self-certify to UA**  
**Standard 1200, and Reliability Coordinators**

Requirement	End of 2 <sup>nd</sup> Qtr 2007		End of 2 <sup>nd</sup> Qtr 2008		End of 2 <sup>nd</sup> Qtr 2009		End of 2 <sup>nd</sup> Qtr 2010	
	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
<b>Standard CIP-002-1 — Critical Cyber Assets</b>								
R1	SC	BW	C	SC	AC	C	AC	AC
R2	SC	BW	C	SC	AC	C	AC	AC
R3	SC	BW	C	SC	AC	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC

# Implementation Plan – Table 1<sup>A</sup>

- Table 1<sup>A</sup> – **System Control Centers** for BA, TOP, RC that were required to self certify to the UA 1200

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
7/1/2008	28 Requirements	13 Requirements*	
7/1/2009		28 Requirements	13 Requirements
7/1/2010			41 Requirements

\* Requirements listed in the “System Control Center” column of Table 1 in the Implementation Plan

# *The First 13...*

---

- CIP-002
  - R1, R2, R3
- CIP-003
  - R1, R2, R3
- CIP -004
  - R2, R3, R4
- CIP-007
  - R1
- CIP-008
  - R1
- CIP-009
  - R1, R2

*Note that CIP-005 (Electronic Security Perimeter) and CIP-006 (Physical Security) have no “Compliant” requirements for the 6/30/08 deadline*

*Also note that compliance to CIP-001 is already required*

# *CIP-001 – Sabotage Reporting*

---

- Confusing for many...
- Sabotage *IS* intentional disruption of operations (even if intent is suspected)
- Sabotage *IS NOT* vandalism or theft
- Have identification/handling procedures
- **Know** your LEA, FBI and DHS contacts; more than just their phone number
- Provide documented proof of relationships and agreements

# CIP-002 – CCA Identification

---

- R1: Adopt a methodology
  - NERC RAWG Guideline **[DRAFT]**
    - Following NERC ANSI standards process (very slow)
  - Will likely hold WECC workshops end of May 2008
- R2: Critical Asset List
  - Start with all facilities that are part of the BPS
  - Impact Analysis vs. Risk-Based Methodology
  - Risk to the BPS is the real question
  - Redundancy doesn't count
- R3: Critical Cyber Asset List
  - Don't forget Decision Support Systems
  - EMS, DCS, RTUs, IEDs, PLCs, Relays
  - Redundancy doesn't count

# *CIP-003 – Security Mgmt Controls*

---

- R1: Have specific policy for CIPS
  - Generic policy might not suffice
  - Include provisions for emergency situations
  - Make it available to all applicable personnel
- R2: Name Senior Management Official
  - The higher in the org-chart the better

# *CIP-004 – Personnel and Training*

---

- R2: Annual Training
  - Employees, contractors and service vendors
- R3: Personnel Risk Assessment
  - ID verification
  - 7-year criminal history
- R4: Access Control
  - Must know who has access to what and when
  - Have access revocation procedures
- *Keep good records*

# *CIP-007 – Systems Security Mgmt*

---

- R1: Test Procedures
  - Follow test and change control procedures before attaching any device inside the ESP
  - Test environment must reasonably mirror production environment
  - Document test results

# *CIP-008 – Incident Response*

---

- R1: Incident Response Plan
  - Procedures to characterize and classify events as reportable incidents
  - Actions, roles and responsibilities of response teams and communication plans
  - Process for sharing incident information with ES-ISAC
  - Annual documentation review and test

# *CIP-009 – Recovery Plans*

---

- R1: Recovery Plans

- Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s)
- Define the roles and responsibilities of responders

- R2: Exercises

- Test recovery plan at least annually

# *WECC CIP Outreach*

---

- Open Mic calls dedicated to CIP issues
- Email CIP questions to [pmiller@wecc.biz](mailto:pmiller@wecc.biz)
- CUG Meetings
- CIPUG
- Workshops on specific standards
- Dedicated Cyber Security page on website
- Living Cyber Security FAQ on website

# *Cyber Security Webpage*

---

- **WECC Cyber Security**

- Mission statement(s) - WECC's Cyber Security commitment
- Cyber Security related items on the WECC Calendar (compliance dates, open mic calls, training, outreach, etc)
- Submit a Cyber Security question
- FAQ for common security questions to WECC
- WECC Cyber Security blog/news-headlines
- All WECC Security guidelines and policies

- **Cyber Security Regulations and Standards**

- NERC CIP Standards
- FERC Order 706

# Cyber Security Webpage

---

- **Forums, Working Groups and Committees**

- WECC: CIPUG, CUG, PSWG, DEWG, EMSWG
- NERC: CSSWG, CIPC
- DHS: PCSF, US-CERT ES-Portal
- Industry: E-Sec NW, EEI Security Committee, APPA

- **Useful Cyber Security Resources**

- NERC ES-ISAC (includes all guidelines as well as RAMs, etc)
- NIST SP800 series
- ISA-SP99
- ISO27001
- US-CERT
- Cyber Security Procurement Language for Control Systems
- National Labs: PNL, INL, SNL
- Find your local FBI contact
- Find your local DHS PSA

# *CIP Auditor Training*

---

- All Regional Entities are being trained
- Training is developed by NERC and SMEs from the RROs
- Following the GAGAS (“Yellow Book”) standards for performance audits
- No Registered Entity training expected
  - Use the RSAWs and Yellow Book
  - Get trained by ISACA and IIA

# *CIP RSAW*

---

- First cut will be only for the first 13 requirements (7/1/08)
- Being developed by NERC and SMEs from the RROs
- Should be “draft complete” after 5/1/08
- Will continue to evolve with **your input** over time until Auditably Compliant stage (7/1/09)

# *CIP Compliance Overview*

---

- **[BW, SC]** Before Compliant stage, semi-annual self-certifications will be conducted
- **[C]** Compliant Stage (on or after 7/1/08)
  - All CIP Standards will be included in the Actively Monitored list of standards
  - Only self-certification, self-reports, investigations
  - No audits or spot-checks until AC stage
- **[AC]** Auditably Compliant Stage (on/after 7/1/09)
  - Subject to audits and spot checks

# *Pre-Compliant Stage*

---

- **Begin Work (BW)** - Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements
- **Substantially Compliant (SC)** - Entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant

# *Semi-Annual Self-Certifications*

---

- Between now and “Compliant” stage
- Beginning July 1<sup>st</sup>, 2008 – on self-certification:
  - 28 requirements from Table 1<sup>A</sup>
  - 40 requirements from Table 1<sup>B</sup>
  - 40 requirements from Table 2
- Beginning December 31<sup>st</sup>, 2008 – on self-certification:
  - 40 requirements from Table 3
- Semi-Annual self-certifications to start July 1<sup>st</sup> and January 1<sup>st</sup>; starting July 1<sup>st</sup>, 2008
- WECC will be following up on inconsistent/insufficient responses **and non-response** to prior self-certifications

# *Semi-Annual Self-Certifications*

---

- WECC will send the semi-annual self-certification forms to the Registered Entities (applicability based on CIP Implementation Plan)
- A Registered Entity indicating it has not reached the milestone for a requirement will be required to submit a mitigation plan

# *Compliant Stage*

---

- Compliant (C) - Entity meets the full **intent** of the requirements and is beginning to maintain required “data,” “documents,” “documentation,” “logs,” and “records”

# *Compliant Stage - Monitoring*

---

- Self-Reporting – Registered Entity is to report when they are not compliant with a requirement
- Self-Certification – Beginning July 1, 2008, there will be 13 requirements from the CIP Implementation Plan Table 1A, and 1 requirement from Table 1A, and Table 2, the Registered Entity must self certify they are compliant with the each requirement.
  - Beginning December 31, 2008, registered entities in Table 3 must self-certify that they are compliant with the 1 requirement.
- The Self-Certification process will be managed so that the Self-Certification is sent to the Registered Entity by WECC within an agreed upon time frame.
- Investigations – For cause due to an event, complaint, report or other identified by other means

# Implementation Plan – Table 1<sup>A</sup>

- Table 1<sup>A</sup> – **System Control Centers** for BA, TOP, RC that were required to self certify UA 1200

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
7/1/2008	28 Requirements	13 Requirements*	
7/1/2009		28 Requirements	13 Requirements
7/1/2010			41 Requirements

\* Requirements listed in the “System Control Center” column of Table 1 in the Implementation Plan

# Implementation Plan – Table 1<sup>B</sup>

- Table 1<sup>B</sup> – **Other Facilities** for BA, TOP, RC that were required to self certify UA 1200

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
7/1/2008	40 Requirements	1 Requirement*	
7/1/2009		39 Requirements	2 Requirements
7/1/2010			41 Requirements

\* CIP-003.R2 – Leadership; found in the “Other Facilities” column of Table 1 in the Implementation Plan

# Implementation Plan – Table 2

- Table 2 – TSP, those BA and TOP Not Required to Self-certify to UA Standard 1200, NERC, and Regional Entities

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
7/1/2008	40 Requirements	1 Requirement*	
7/1/2009		40 Requirements	1 Requirement
7/1/2010			41 Requirements

\* CIP-003.R2 – Leadership; found in the “All Facilities” column of Table 2 in the Implementation Plan

# Implementation Plan – Table 3

- Table 3 – IA, TO, GO, GOP, and LSE

Date	Substantially Compliant Stage	Compliant Stage	Auditably Compliant Stage
12/31/2008	40 Requirements	1 Requirement*	
12/31/2009		40 Requirements	1 Requirement
12/31/2010			41 Requirements

\* CIP-003.R2 – Leadership; found in the “All Facilities” column of Table 2 in the Implementation Plan

# *Auditably Compliant*

---

- One **full year** of compliance evidence
- Requirements are subject to full CMEP:
  - Audits (on-site and off-site)
  - Spot Checks
  - Self-Report
  - Self-Certification
  - Investigations
  - Periodic Reports
  - Penalties and Sanctions

# *CIP Future*

---

- FERC

- FERC (and HSC) want a more prescriptive and restrictive standard going forward
- NIST 800-53/800-82 may be the goal

- NERC

- SAR for new CIPS drafting teams by 4/4/08
- CIP-010, 011 and 012...

- A security-related event may accelerate changes or new standard development

# *CIP Compliance Tips*

---

- Get the CIP-002 effort done first, then run other initiatives in tandem/parallel where possible
- Leverage Control Systems, Information and Physical Security, and DR/BCP experience
- Design scalable solutions that can expand to meet new standards – *they will change*
- Defense in depth is best; can demonstrate intent
- Don't forget about sensitive information/data
- Talk to your peers and find out what works
- Use the RSAW and Implementation Plan

# Questions?



**Patrick Miller CISA, CISSP-ISSAP**  
**Sr. Compliance Engineer, Cyber Security**  
**Western Electricity Coordinating Council**  
**7600 NE 41<sup>st</sup> Street, Suite 160**  
**Vancouver, WA 98662**  
**360.567.4056 (d) / 503.260.6472 (m)**