



Western Electricity Coordinating Council

WECC CIP Compliance Update

E-Sec NW 2008-Q1 Compliance Workshop
Two World Trade Center, Portland, OR
March 19th, 2008

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

Overview

- WECC CIP Compliance Staff
- Compliance Portal
- Compliance Website
- CIP Outreach
- CIP RSAW
- CIP Training
- CIP Compliance

WECC CIP Compliance Staff

- Patrick Miller
 - CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM
 - 20+ years in IT
 - 8+ years in Energy
 - Former E-Sec NW Chair
 - WECC Sr. Compliance Engineer, Cyber Security (read: CIP Auditor)
- Will likely grow in the future...

Compliance Portal

- Very complex multi-RRO effort
- Under development, but coming soon
- Entities will have their own portal UI
- Security and auditability are paramount
 - Security assessment is scheduled for 4/10/08
- Using a “trusted” provider and host
 - Built on MS technology, but not MOSS
 - Data Center is located in California
- Stand-alone, not part of the public site

Cyber Security Webpage

- **Report Incidents to ES-ISAC**
- **WECC Cyber Security**
 - Mission statement(s) - WECC's Cyber Security commitment
 - WECC's compliance portal (sub links to common documents such as surveys, self-reports, self-certification)
 - Cyber Security related items on the WECC Calendar (compliance dates, open mic calls, training, outreach, etc)
 - FAQ for common security questions to WECC
 - Submit a Cyber Security question
 - 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: PSWG, DEWG, EMSWG [CIPUG, CSWG]
- NERC: CSSWG, CIPC
- DHS: PCSF, US-CERT ES-Portal
- Industry: E-Sec NW
- Industry: EEI Security Committee

- **Useful Cyber Security Resources**

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

WECC CIP Outreach

- Open Mic calls dedicated to CIP issues
- Living FAQ on new website
- Dedicated Cyber Security page on website
- CUG Meetings
- CIPUG/CIPWG/CIPTF?

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” by 5/1/08
- Will continue to evolve with **your input** over time until Auditably Compliant stage
- Expected to be finalized before 7/1/09

CIP Auditor Training

- All Regional Entities are being trained
- NERC has committed to four classes
 - Two in Q4 of 2008; Two in Q1 of 2009
- Being developed by NERC and SMEs from the RROs
- Following the GAGAS (“Yellow Book”) standards for performance audits

CIP Compliance

- Before Compliant stage, semi-annual self-certifications will be conducted
- Compliant Stage (on or after 7/1/08)*
 - The “first 13” requirements will be included in the Actively Monitored list of standards
 - Only self-certification, investigations, periodic reports
 - No audits or spot-checks until AC stage
- Auditably Compliant Stage (on/after 7/1/09)**
 - Subject to audits and spot checks

* 7/1/08, 12/31/08, 7/1/09, or 12/31/09, depending on Entity and Standard, as defined within the Implementation Plan

** 7/1/09, 12/31/09, 7/1/10, or 12/31/10, depending on Entity and Standard, as defined within the Implementation Plan

Semi-Annual Self-Certifications

- Between now and “Compliant” stage
- Beginning July 1st, 2008 – on self-certification:
 - 28 requirements from Table 1A
 - 40 requirements from Table 1B
 - 40 requirements from Table 2
- Beginning December 31st, 2008 – on self-certification:
 - 40 requirements from Table 3
- No sanctions or penalties until Compliant stage for each requirement
- Semi-Annual self-certifications to start July 1st and January 1st; starting July 1st, 2008
- Will be following up on inconsistent/insufficient responses to prior self-certifications

Semi-Annual Self-Certifications

- The Regional Entities 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 explain why milestone was not met.

In response to Registered Entities that reporting via semi-annual self-certification they have not met the CIP Implementation Plan Milestones, the Regional Entity will:*

- Work informally with the Registered Entity or
- Require a Remedial Action Plan to assist the Registered Entity in achieving full compliance

** Note: These activities are outside the CMEP process.*

“Compliant” Stage

- Compliant (“C”) means the entity meets the full intent of the requirements and is beginning to maintain required “data,” “documents,” “documentation,” “logs,” and “records”
- A Registered Entity that indicates it has not met the full intent of a Compliant Stage requirement will be subject to CMEP Processes including Remedial Action Plans

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 the Regional Entities within an agreed upon time frame.
- Investigations – For cause due to an event, complaint, report or other identified by other means

Auditably Compliant

- Requirements are subject to full CMEP:
 - Audits
 - Spot Checks
 - Self-Report
 - Self-Certification
 - Investigations
 - Periodic Reports

Implementation Plan – Table 1A

- Table 1A – 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

* The first 13

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

Implementation Plan – Table 1B

- Table 1B – 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

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

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

Under Construction...

- New staff
- New compliance portal
- New website
- New RSAWs
- Form CIPUG/CIPWG/CIPTF?
- New training for WECC staff
- Please bear with us; we're growing as fast as possible...

Questions?



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