



Western Electricity Coordinating Council

WECC CIPS Update

E-Sec NW CIPS Summit
Doubletree Lloyd Center, Portland, OR
July 22nd, 2008

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

Introduction

- Patrick Miller

- CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM
- 20+ years in IT
- 8+ years in Electric Sector
- Sr. Compliance Engineer, Cyber Security

- *I will be (one of) your WECC CIP Auditor(s)*

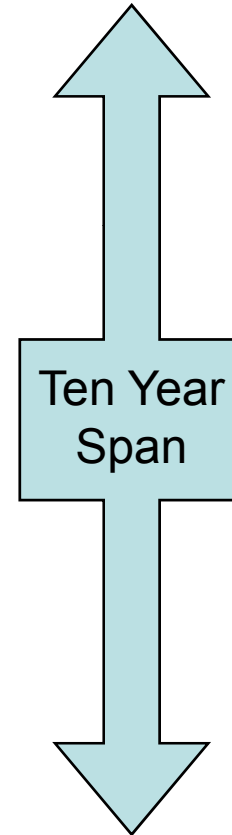
Overview

- CIPS Background
- WECC CIP Compliance Statistics
- WECC Compliance Organization
- WECC CIPS FAQ
- BW, SC and the CMEP
- Regional Consistency
- WECC CIPUG Happenings
- Upcoming WECC CIP Workshops
- CIP Compliance Tips

CIPS Past to Present

- PDD 63
- 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
- FERC Order 706-A

...**05/1998**



...**05/2008**

Influential Factors

- Interdependency studies
- NE Blackout 2003
- “Aurora” DPCD issue
- SANS CIA briefing
- RSA & Ira Winkler
- House Subcommittees
- Chinese Hackers
- Hatch Shutdown
- Project Hydra
- *Hype vs. Reality in the Media*



Geico

WECC CIP Pre July 1 Stats

- Pre July 1 Self Reports
 - 37
- Pre July 1 Mitigation Plans
 - 41
- Still processing

WECC CIP Self-Certification Stats

- Self Report forms submitted by July 15:
 - 272
- Self Report forms not received yet:
 - 105
- Still receiving late submittals

WECC CIP Self-Certifications

- Post July 15 (late) submittals
 - 7

Details per function:

29 BA

167 GO

165 GOP

123 LSE

28 PA

78 PSE

3 RC

47 RP

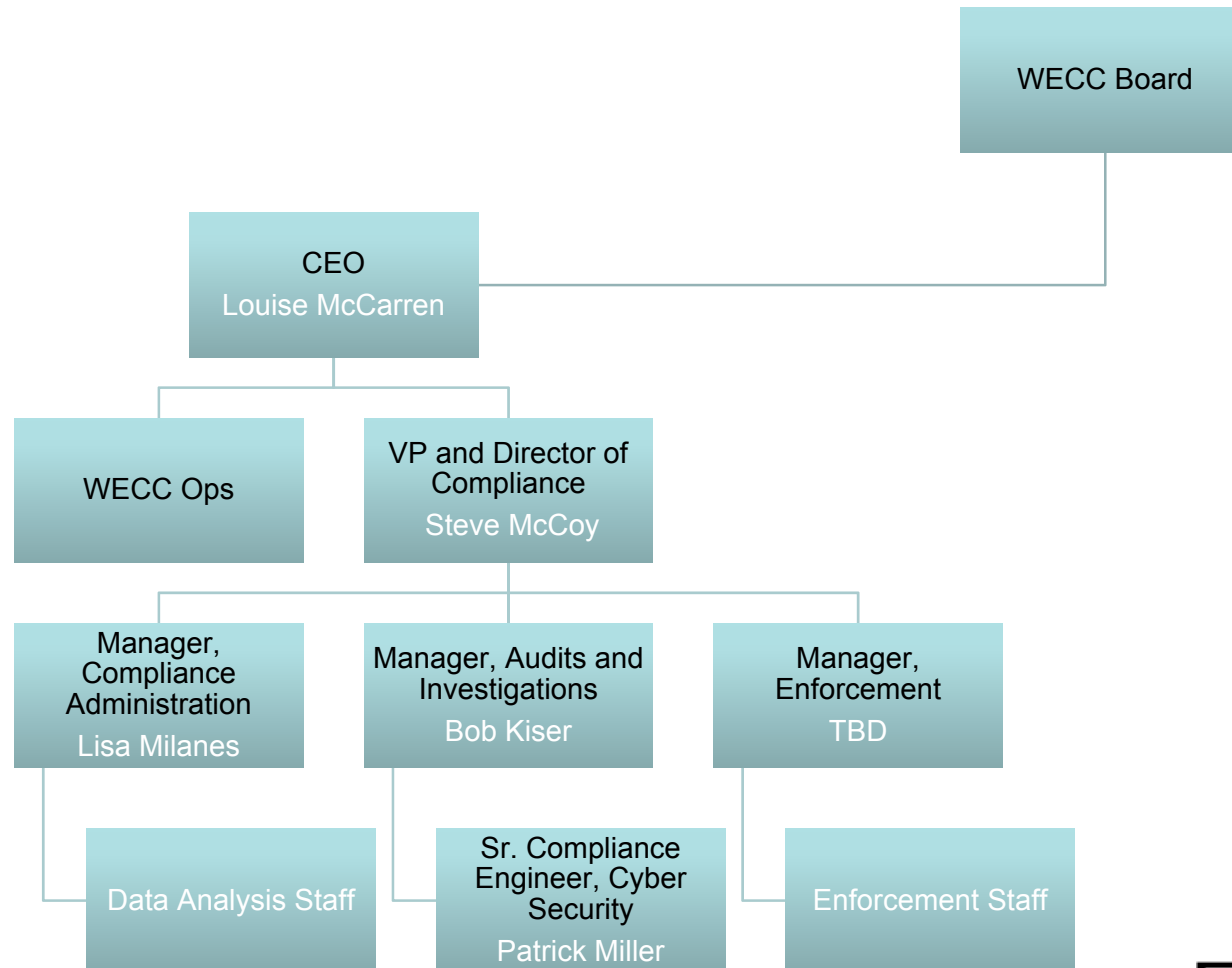
43 TOP

70 TO

40 TP

31 TSP

WECC Compliance Org Structure



CIPS FAQs

- What is annual?
 - One calendar year, +/- one month
- Implementation Plan?
 - Table 1: CIP-003.R1 – SC > AC, 2008 > 2009
 - Table 3: 2006
- Table 1 only vs. multi-function reporting?
 - Unless the facility is defensibly single-function, then Table 1 (for applicable entities)

BW, SC and the CMEP

- BW and SC; no audits, but CMEP applies
- BW and SC auditing process uses the Self-Certification monitoring element of the CMEP
- No Self-Reports or Mitigation Plans are required for BW or SC

Pre-Compliant Stages

- **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

Compliant Phase

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

Compliant Phase - Monitoring

- Requirements are subject to partial CMEP:
 - Spot Checks
 - Self-Report
 - Self-Certification
 - Investigations
 - Periodic Reports
 - Penalties and Sanctions
- No audits (on-site or off-site) until 7/1/09

Auditably Compliant Phase

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

Regional Consistency

- RECM
 - Regional Entity Compliance Managers
- CIPM WG
 - CIP Managers Working Group
- AOT
 - NERC Audit Observation Team
- Attendance at each other's workshops...

CIPUG Distribution List Issues

- Migration to Exchange 2007
 - Some names were dropped
 - List permissions changed
- Email sent to list was distributed to all
 - Out of office notifiers replied back to list
 - Email echo/bounce-back storm happened
- CIPUG list was disabled
- Send request to cnoorda@wecc.biz to be re-added to the list

CIPUG Table 13 Workshop Notes

- Issues that will be addressed in future events:
 - Simple logistics: more microphones, better food, more beverage options, power strips
 - Split technical and non-technical events
 - Workshops specific to a single standard
- **Biggest request was/is for examples**
 - But WECC can't give examples, so...

Upcoming Workshops

- CIP-005 – Electronic Security Perimeter Workshop
 - November 12th, 2008
 - Hilton Downtown, Portland, OR
- CIP-006 – Physical Security Perimeter Workshop
 - December 17th, 2008
 - Marriott Coronado, San Diego, CA
- CIP-007 – Systems Security Management Workshop
 - January 15th, 2009
 - Marriott Buttes, Tempe, AZ
- Auditably Compliant Ramp-Up
 - February 10th – 11th
 - Hilton Downtown, Salt Lake City, UT

CIP-005 – ESP Workshop

- November 12th 2008; 8:00AM – 4:00PM
- Hilton Downtown, Portland, OR
- Two panels: asset owners and consultants
- Asset owners will walk through CIP-005
- Consultants (vendors) will provide feedback
- Consultants will be required to remain anonymous unless approached directly
- **WECC is not endorsing any approach, model, consultant, vendor, etc**

CIP Compliance Tips

- Build a cross-functional team
 - Leverage Control Systems, Information and Physical Security, and DR/BCP experience
 - Listen to them and send their message upstream

- Don't attach everything to the CIPS effort
 - Not everything is tied to compliance
 - Can erode credibility
 - Non-CIPS good security is still a good idea

CIP Compliance Tips

- Automate where you can; use technology
 - Manual processes and technology can both fail but technology doesn't take vacations
 - Don't forget to monitor systems
- Be sensitive to Control Systems nuances
 - IT models may need to flex
 - Respect perspectives from both camps

CIP Compliance Tips

- Design scalable solutions that can expand to meet new standards – they will change
 - Don't re-invent the wheel for every shift
 - Don't settle for the minimum

- Step over the line
 - The closer you are to the line, the higher the necessary magnification on the microscope
 - Make it obvious, transparent and simple

CIP Compliance Tips

- Documentation is important!
 - Every word counts
 - Match language and documentation to standards wherever possible
- Change the way you do business
 - Don't just patch together existing documents
 - Demonstrate a true shift toward a more secure posture

CIP Compliance Tips

- Go beyond your SOC efforts for your Internal Compliance Program
 - WECC/NERC does not audit 888/889/890
 - Use what works, but don't stop there
 - You may need special programs and special documentation that just speaks to 693/706
 - Market, Generation and Transmission all need to have functional CIP programs
 - WECC will audit you as one company

CIP Compliance Tips

- Talk to each other and WECC
 - You don't have to re-invent the wheel
 - Share what works and what doesn't
 - Establish contacts for questions and info
 - CIPUG – email cnoorda@wecc.biz to join
 - CIPWG – email dick.robert@chelanpud.org
 - WICF – www.wicf.biz
 - E-Sec NW – www.esecnw.org

Get Involved

- Join the NERC Standards Mailing List
 - Latest information about Reliability Standards
 - Send your request to lauren.koller@nerc.net
 - Make the subject of your message Subscribe to Standards Mailing List
 - Include any e-mail address(es) you wish to have added to the list in the body of the message if different than your "From" address

Get Involved

- Request formal interpretations
- Initiate your own SAR
 - NERC Rules of Procedure
 - http://www.nerc.com/~filez/rules_of_procedure.html
 - Appendix 3A
 - ftp://ftp.nerc.com/pub/sys/all_updl/rop/Appendix3A_StandardsDevelopmentProcess.pdf
- Nominate yourself/others for drafting teams
 - Cyber Security (Project 2008-06)
 - http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html

Get Involved

- **Provide comments to NERC and FERC**

- CIP-006.R1.1 (Progress Energy)

- http://www.nerc.com/~filez/standards/Project2008-10_CIP-006_RFI_Progress.html

- Everyone can do at least this much!

- *If you don't get involved and participate, you can't complain about the situation...*

What About the Money?

- NARUC positions
 - CIP Committee is regularly briefed
 - Documents issued: cost recovery, CIP issues and ratecase manual
- Others will likely follow suit, but may need to be shown the precedent already set
- Conflict for Munis
 - Standards are not about the customer
 - May not fit well within political arena

CIP Crystal Ball – NERC

- Will the CIPS standards be drafted or refined differently this time?
- Will they resemble NIST 800?
- CIP-010, 011 and 012?
 - Comm (protocols & links), Physical, Market Systems?
- Sergel's new security direction?

CIP Crystal Ball – FERC

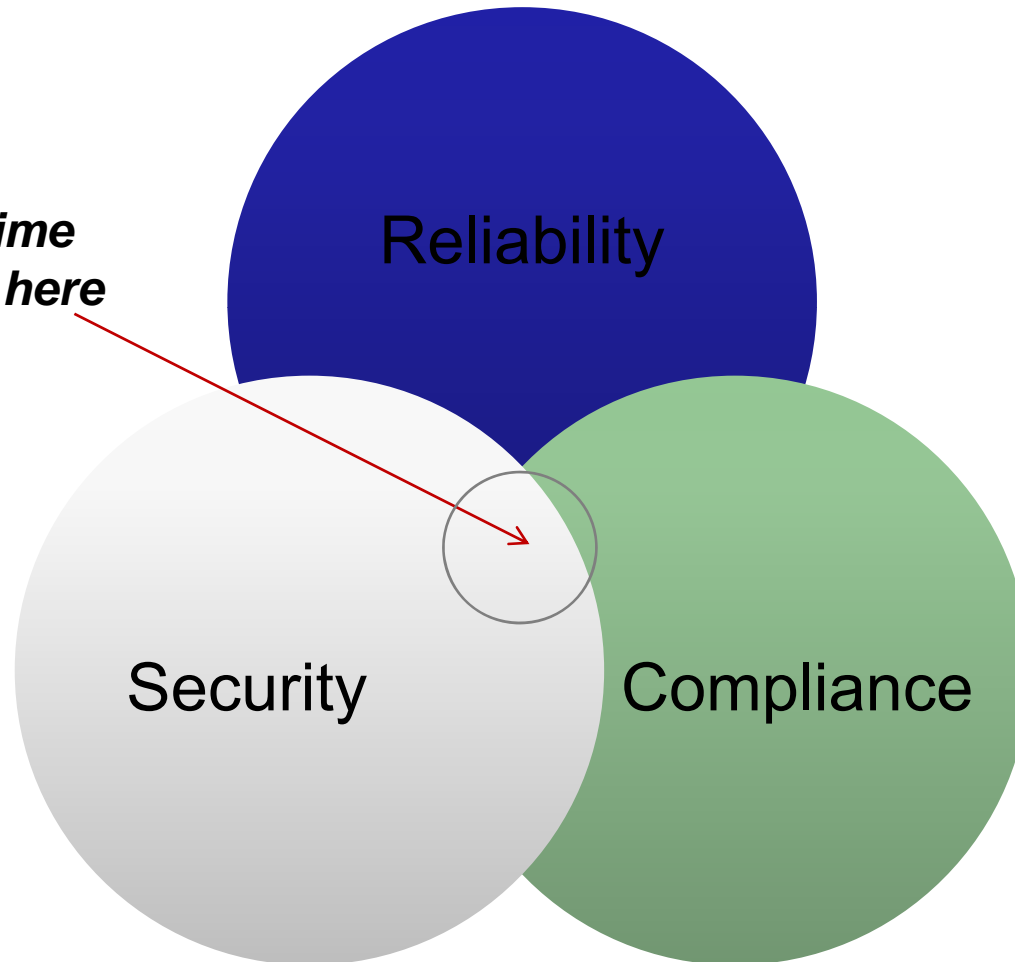
- FERC (and HSC) want a more prescriptive and restrictive standard going forward
- FERC requested additional authority to create standards in emergency threat situations
- Subcommittee request has already been sent by Rep Langevin
- Something resembling FISMA/FIPS (NIST 800-53, 800-82) appears to be the goal

CIP Crystal Ball – Industry

- Perfect Storm...
 - Technology shift
 - New vulnerability research focus
 - Aurora and others?
 - Media
 - Congressional interest
- New standards from different agencies
- Put on your seatbelt and remain seated...

The Big Picture

*Put your time
and money here*



Questions?



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