



Western Electricity Coordinating Council

CIP-008/009 Workshop

WECC Critical Infrastructure Protection User Group (CIPUG)
The Grove Hotel, Boise, ID
March 18th, 2009

Disclaimer

The Western Electricity Coordinating Council (WECC) makes no representation as to the accuracy or completeness of the information contained herein or otherwise provided by WECC, their affiliates or third parties, and accept no responsibility or liability, in contract, in tort, in negligence, or otherwise, should the information be found to be inaccurate or incomplete in any respect. WECC is not acting as an advisor to the recipient of this information, and the ultimate decision to proceed with any action rests solely with the recipient of this information.

Therefore, prior to entering into any action, the recipient of this information should determine, without reliance upon WECC, the economic risks and merits, as well as the legal, and accounting characterizations and consequences, of the transaction and that it is able to assume these risks.

Thanks For Attending!

- Fire exits are...
- Restrooms are...
- Lunch will be around...
- Please **use a microphone**...
- Please **no recording** equipment...
- Please **silence** all cell phones, mobile devices, laptops...

WECC Staff

- Compliance

- Bill Fletcher – Compliance Engineer, CIP
 - 360.567.4061
 - wfletcher@wecc.biz
 - <https://twitter.com/williamfletcher>
- Patrick Miller – Sr. Compliance Engineer, CIP
 - 360.567.4056
 - pmiller@wecc.biz
 - Blackberry PIN: 31F2495F
 - <https://twitter.com/patrickcmiller>

WECC Staff

- Outreach
 - J. Taud Olsen – Director, Stakeholder Relations and Compliance Outreach
 - tolsen@wecc.biz
 - 801.819.7603 (desk)
 - 801.883.6894 (mobile)
- Logistics *[special thanks!]*
 - Becky Hudson
 - Melanie Wood

CIPUG Website

The screenshot displays the WECC Compliance website. At the top, the WECC logo is on the left, and navigation links (Compliance Home, WECC Home, Quick Links, Staff Directory, RMS, Portal Login) are on the right. Below the logo is the text "Western Electricity Coordinating Council". A large "Compliance" header is on the right. A horizontal menu contains: Entity Registration, Reliability Standards, Compliance Library, Audits & Investigations, Enforcement, and Outreach. The Outreach section is active, showing a sidebar with a menu where "Critical Infrastructure Protection User Group (CIPUG)" is selected. The main content area is titled "Outreach Home" and contains a paragraph about WECC's Outreach Plan, followed by a list of links: Compliance User Group (CUG), Open Mic Sessions, Critical Infrastructure Protection User Group (CIPUG), Subject Matter Experts, Compliance Q & A, Western Interconnection Compliance Forum (WICF), Contact Taud Olsen, and View Compliance Calendar. Two red arrows point to the "Outreach" menu item and the "Critical Infrastructure Protection User Group (CIPUG)" menu item.

Compliance Home | WECC Home | Quick Links | Staff Directory | RMS | Portal Login

WECC
Western Electricity Coordinating Council

Compliance

Entity Registration | Reliability Standards | Compliance Library | Audits & Investigations | Enforcement | Outreach

Outreach Home
Compliance Bulletins
▶ Compliance User Group (CUG)
▼ **Critical Infrastructure Protection User Group (CIPUG)**
 • About CIPUG
 • Upcoming Events
 • Previous Workshops
▶ Open Mic
▶ Web Portal Training
Subject Matter Experts
Compliance Q & A
Regional Entities Common Website
WICF
Contact Taud Olsen

Outreach -> Outreach Home

Outreach Home

WECC values the membership of and relationship with each and every member and Registered Entity. In an effort to strengthen stakeholder relations, improve communications, promote meaningful training and education opportunities while providing compliance assistance, WECC's Outreach Plan, led by Taud Olsen, Director of Stakeholder Relations and Compliance Outreach, will focus on the following:

Compliance User Group (CUG)

Open Mic Sessions

Critical Infrastructure Protection User Group (CIPUG)

Subject Matter Experts

Compliance Q & A

Western Interconnection Compliance Forum (WICF)

Contact Taud Olsen

View Compliance Calendar

<http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=100>

CIP Outreach

- CIP-003, April 14th, Denver
- CIP-004, May 6th, Albuquerque
- CIP Open Mic(s), June TBD
- CIPUG/ESEC Summit, Summer, Seattle

- Join the CIPUG email distribution list
 - Send subscribe request to itsupport@wecc.biz

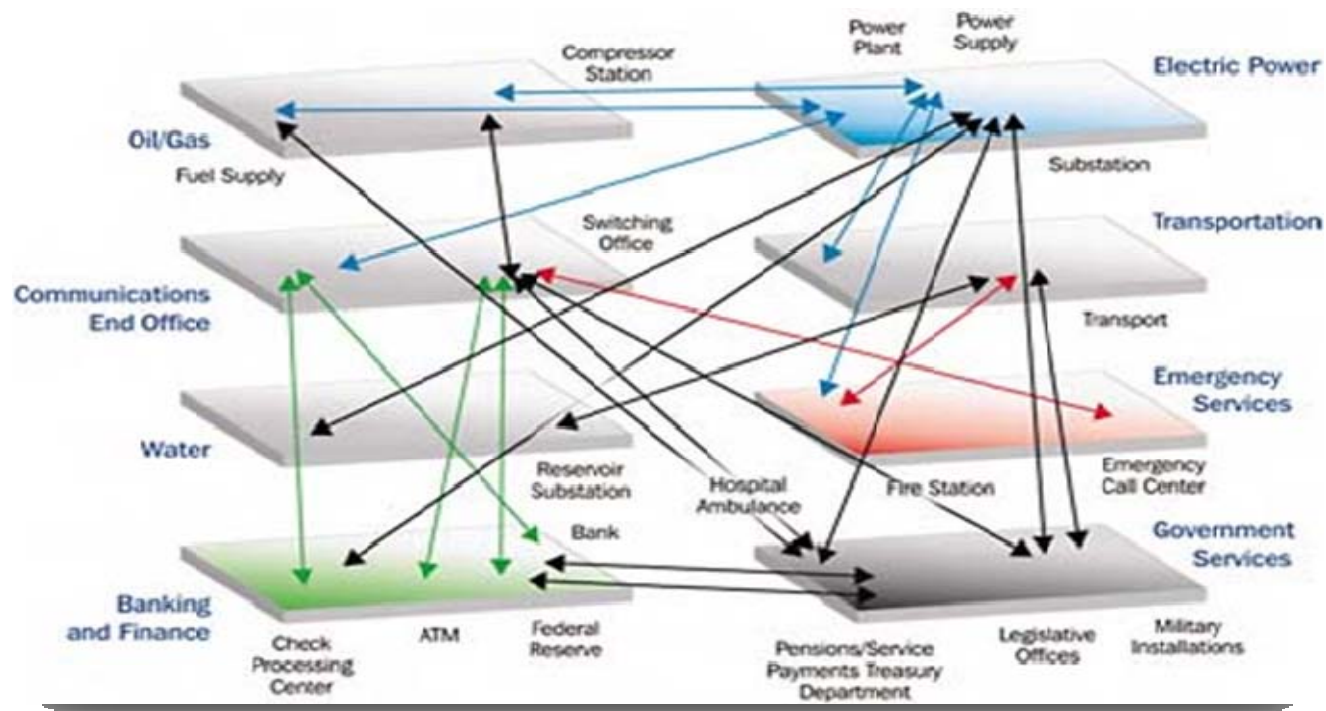
WECC CIPUG Workshops

- #1 request was for examples
 - WECC audit can't do that, but *you* can
- New CIPUG workshop model...
 - Asset owner volunteer panel walks through their organization's implementation
 - Industry expert panel of consultants and vendors provides feedback
 - Audience participation is strongly encouraged
- Webex suggestions?

CIP-008/009 Purpose(s)

- CIP-008 Cyber Security Incident Response Plan
 - “..Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets....”
- CIP-009 Recovery Plan(s) for Critical Cyber Assets
 - “.. Purpose: Standard CIP-009 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....”

Why Have 008/009 Plans?



Source: Previous NIPP plans & National Research Council Publication
http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm

Industry Expert Panelists

- Jim Mapes
- Mark Simon
- David Baker
- Bill Addington
- Bryan Geraldo
- Eric Trapp
- Please feel free to approach them directly during breaks, lunch and after the event

Asset Owner Presenters

- Richard Pace, Southern California Edison
- Barry Jones, San Diego Gas and Electric
- Mike Espinoza, San Diego Gas and Electric

- Please thank them for volunteering for this event!

Warm Up Exercise

- Open survey-style questions/discussion
- Can be filled out in hardcopy
- Can also be emailed to Richard directly
 - Richard.Pace@sce.com
- Results will be sanitized of any attributable information and posted on WECC CIPUG website as additional documentation from this workshop

Survey...

1. CIP-009 Purpose states that the plans follow "established business continuity and disaster recovery techniques and practices". Do you already have a business continuity program in place at your business?
2. Does your business have an established disaster recovery organization? If not, where does this skill set reside?

Survey...

3. By percentage, how much of your now-identified CCAs already had disaster recovery solutions in place prior to NERC CIP?
4. In the last 3-5 years, has your business ever had to invoke your business continuity or disaster recovery plans? What were your experiences?

Survey...

5. Is your business using a planning tool to assist with disaster recovery or business continuity plan development? Which tool and how has it performed for you?
6. How are you addressing R1's requirement to "specify the actions in response to events or conditions of varying duration and severity"?

Survey...

7. Are you writing your BC or DR plans to address hazards specific to your area of operation (earthquake, fire, flood, etc.)?
8. Although it's not a CIP-009 requirement, are you also storing your backup media offsite from your data centers?
9. What has been your experience in working with vendors to establish DR solutions over the past year to comply with CIP-009 requirements?

CIP-008/009 Schedule

- Table 1
 - Part of the “First 13”
 - Compliant (C) by July 1st, 2008
 - Auditably Compliant (AC) by July 1st, 2009
- Table 2
 - Compliant (C) by July 1st, 2009
 - Auditably Compliant (AC) by July 1st, 2010
- Table 3
 - Compliant (C) by January 1st, 2010
 - Auditably Compliant (AC) by January 1st, 2011

Spirit vs. Letter

- You will be audited against the letter, *but...*
- Immediately apparent or microscope?
- Keep it simple (Ockham's Razor)
- Keep it separate
 - Watch for dependencies
- Think beyond the letter
 - What if?
- Be prepared for investigations, just in case

Its All About...

- The audit is not about...
 - The quality or security value of the design
 - Technology or platform preferences
 - Academics or theory
 - Probability, budget or convenience
- The audit is about...
 - Accountability
 - Transparency
 - Consistency
 - Sustainability

CIP Evidence 101 – Do

- Evidence Dos:
 - Connect the dots in advance; try on my hat
 - Balance the details; moderation is good
 - Redact where appropriate
 - Common format
 - Human readable
 - Checksums (hashes; SHA256)
 - Automate whenever possible
 - Follow CIP-003.R4, R5

CIP Evidence 101 – Don't

- Evidence Don'ts:
 - Please, no sensitive information without appropriate protections; **when in doubt, ask**
 - The “dump truck” factor
 - Is this the stuff you're looking for?
 - “Follow all NERC Regulations” bucket
 - Here it is, but you'll need *[insert proprietary product X]* to read it

CIP-008/009 Evidence

- What type of evidence is best?
 - Yes. Yes it is.
 - No, really...
 - Word, Visio, Excel, PDF
 - System/event logs
 - Database reports
 - Packet captures
 - Observations
 - Pretty much anything

Sustaining Compliance

- Make compliance immediately apparent
- Be able to demonstrate the “5 Ws”
- Be able to **tell** the auditor how you meet the requirement (protocol)
 - Often policy, process, procedure, etc
- Be able to **show** the auditor that you are actually meeting the requirement (proof)
 - Often supporting evidence such as logs, spreadsheets, documents, database extracts, captures, etc

Third Party Resources

- Be careful: time and money are scarce
- A well-crafted RFX can help
- Services
 - Everyone is an expert; ask around
 - ...it reminds me of a Dilbert cartoon
- Products
 - Nothing is 100%, all-in-one, total
 - Some options are emerging

Self Reports and Mitigation Plans

- Violations are per Requirement
- Self Reports and Mitigation Plans can identify the Sub-requirement violated
- Be very clear and very detailed
 - Dates, systems, processes, etc mapped directly to the Requirement/Sub-requirement violated
- Don't forget to include the VRF (and VSL)!
- Provide ALL evidence necessary
- Again, be mindful of sensitive information

CSO706SDT = CIP v2*

- The CIP v2 Horizon
 - If you are still designing, factor in v2
 - If you are not still designing, start incremental changes to arrive at v2 on time
- Stay in the loop** ...
 - CSO706SDT “Plus”, CIPC, E-SEC, EEI, WICF, SANS, etc
 - **Comment!**

* http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

** http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

CIPS v2 Pre-Ballot Window

- **Revisions to Cyber Security Standards CIP-002-1 through CIP-009-1 (Project 2008-06)**
- **CIPS Ballot Pool and 30-day Pre-ballot Window**
 - March 3 – April 1, 2009
 - Registered Ballot Body members may join the ballot pool to be eligible to vote on these standards revisions **until 8 a.m. EDT on April 1, 2009**
 - <https://standards.nerc.net/BallotPool.aspx>

CIPS v2 Target Dates

- Ballot Round One
 - April 1st through April 10th
 - At least one negative vote and comments are expected, which would prompt round two...
- Ballot Round Two
 - April 27th through May 7th
- NERC BOT approval – [late] May 2009
- Submit to FERC – June 2009

*CIP v2 Implementation Plan**

- Will be auditing against v2 upon respective dates specified in the Implementation Plan
- V2 may accelerate compliance deadlines
 - ...The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).
 - Newly registered entities** must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

* http://www.nerc.com/docs/standards/sar/Implementation_Plan_V2_Cyber_Security_Standards_2008Nov20.pdf

** http://www.nerc.com/docs/standards/sar/New_Asset_Implementation_Plan_2008Nov20.pdf

CIP v3

- Drafting team from v2 is already chartered (per SAR) to begin drafting v3
- Early discussions include:
 - Serial and other protocols
 - Encryption
 - Forensics
 - Alignment with NIST
 - Many other substantive changes

CIP Violation Severity Levels (VSLs)

- Current CSO706 Drafting Team is working on the VSLs
 - Larry Bugh of RFC is leading effort
- Should be available for comment soon
- Will need to be complete before 7/1/09

Technical Feasibility Exceptions

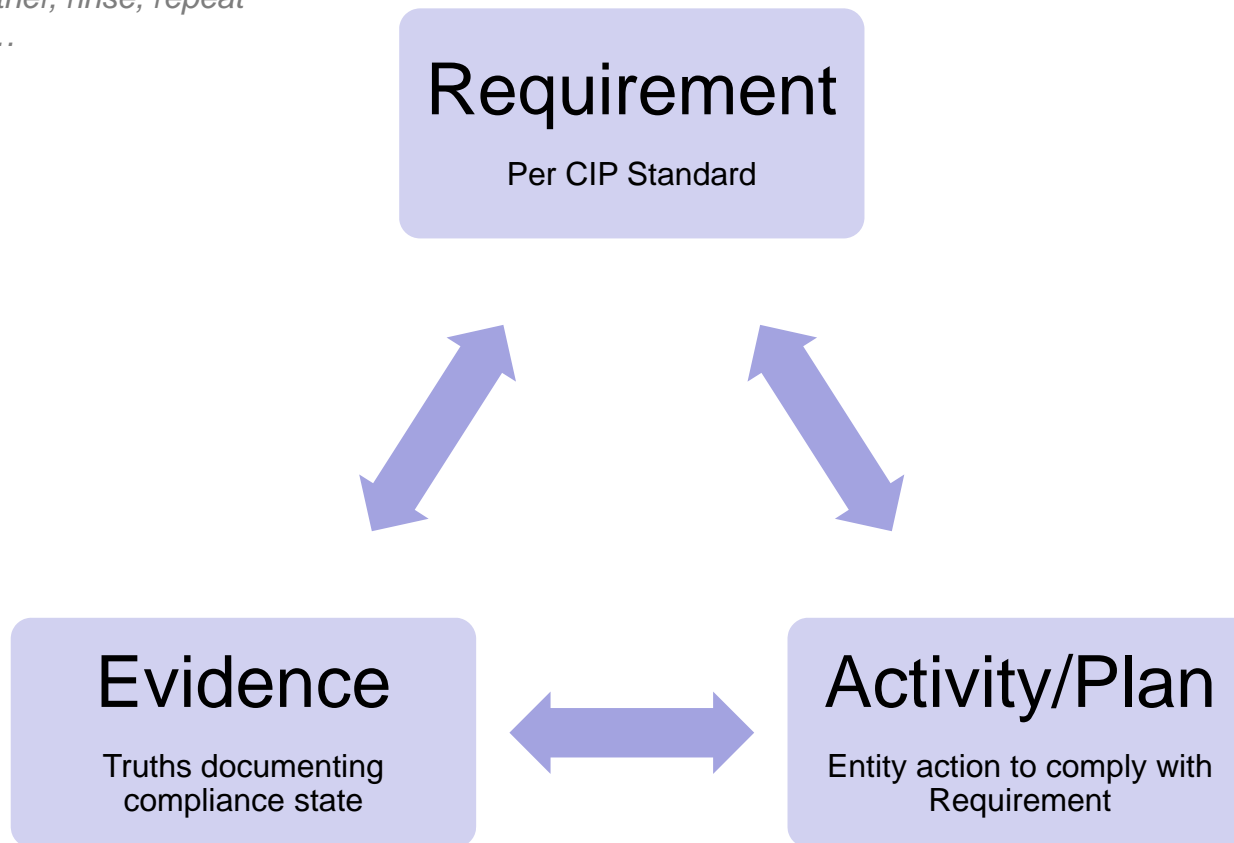
- Per Order 706, TFEs must be addressed appropriately
- Proposed as Appendix 4D of NERC Rules of Procedure
- Should be posted for comment March 13th for 45 day window
- Please comment!

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 – yet...
 - Use the RSAWs and Yellow Book
 - Get trained by ISACA and IIA

Perpetual Compliance Cycle

A.K.A. – lather, rinse, repeat
or HWoD...



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
360.567.4056

Bill Fletcher
Compliance Engineer, Cyber Security
Western Electricity Coordinating Council
7600 NE 41st Street, Suite 160
Vancouver, WA 98662
wfletcher@wecc.biz
360.567.4061