



Western Electricity Coordinating Council

# *2009-2010 CIP Spot Check & Audit Approach*

---

WECC Critical Infrastructure Protection User Group (CIPUG)  
Albuquerque Marriott, Albuquerque, NM  
May 5<sup>th</sup>, 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...

# CIPUG Website

The screenshot shows the WECC Compliance website. The top navigation bar includes links for Compliance Home, WECC Home, Quick Links, Staff Directory, RMS, and Portal Login. The main header features the WECC logo and the word "Compliance". Below the header is a menu with categories: Entity Registration, Reliability Standards, Compliance Library, Audits & Investigations, Enforcement, and Outreach. The Outreach section is expanded, showing a sidebar with links to Outreach Home, Compliance Bulletins, Compliance User Group (CUG), Critical Infrastructure Protection User Group (CIPUG), Open Mic, Web Portal Training, Subject Matter Experts, Compliance Q & A, Regional Entities Common Website, WICF, and Contact Taud Olsen. The main content area displays the "Outreach Home" page, which includes a paragraph about WECC's Outreach Plan and 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)" link in the sidebar.

<http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=10>

0

# *WECC Staff*

---

- Outreach

- J. Taud Olsen – Director, Stakeholder Relations and Compliance Outreach
  - [tolsen@wecc.biz](mailto:tolsen@wecc.biz)
  - 801.819.7603 (desk)
  - 801.883.6894 (mobile)

- Logistics

- Becky Hudson

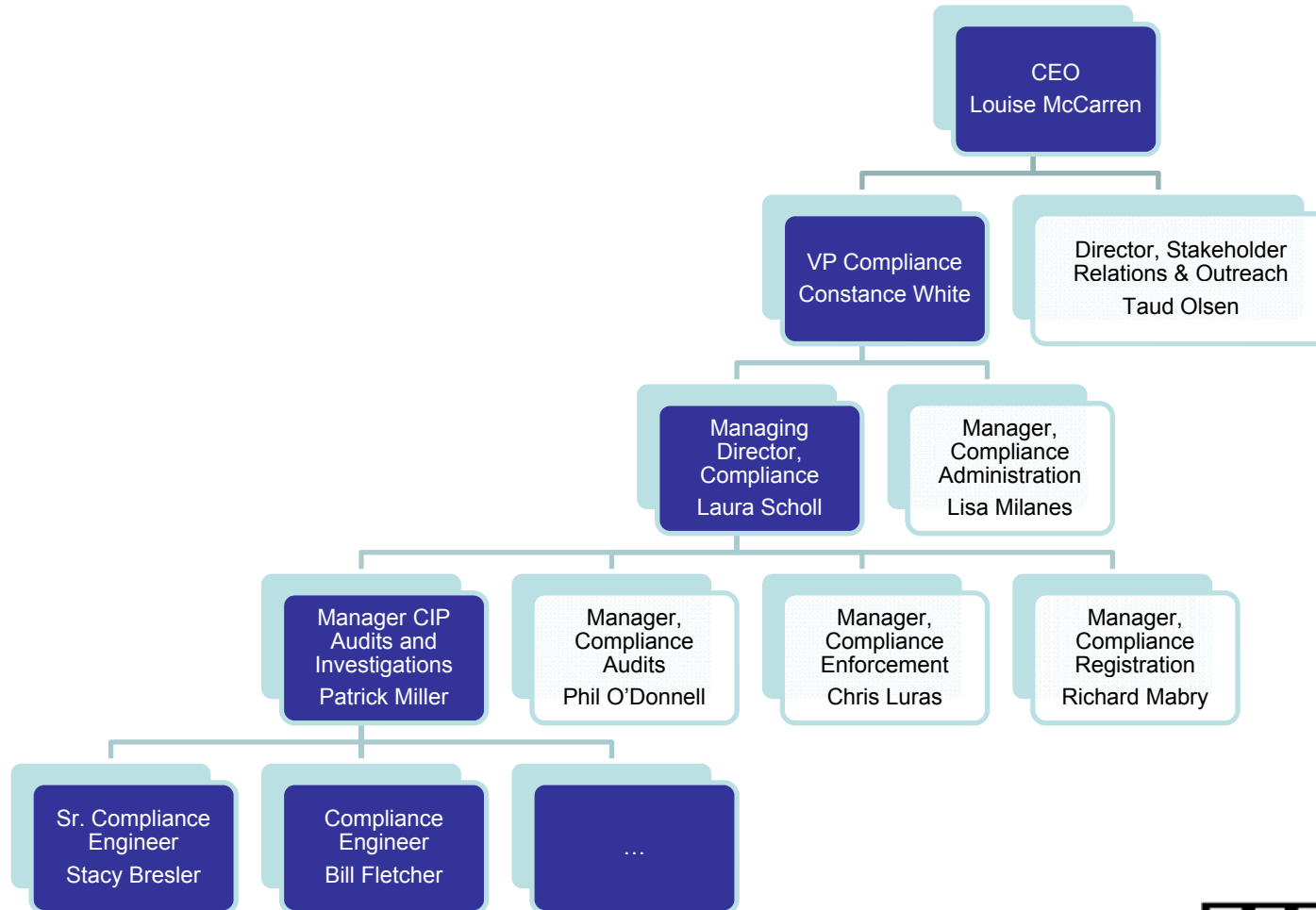
# *WECC Staff*

---

- **CIP Compliance**

- **Bill Fletcher – Compliance Engineer, CIP**
  - 360.567.4061 | [wfletcher@wecc.biz](mailto:wfletcher@wecc.biz)
  - <https://twitter.com/williamfletcher>
- **Stacy Bresler – Sr. Compliance Engineer, CIP**
  - 360.567.4058 | [sbresler@wecc.biz](mailto:sbresler@wecc.biz)
  - BlackBerry PIN: 307890F0
  - <https://twitter.com/stacybre>
- **Patrick Miller – Manager, CIP Audits & Investigations**
  - 360.567.4056 | [pmiller@wecc.biz](mailto:pmiller@wecc.biz)
  - BlackBerry PIN: 31F2495F
  - <https://twitter.com/patrickcmiller>

# CIP Compliance Organization



# *Monitoring: Pre-Compliant (BW, SC)*

---

- Not subject to CMEP:
  - Self certification (survey) requested
- Not bound to CMEP until C phase
- Audits may not begin until AC phase
- No self reports or mitigation plans are due during the BW or SC phases
- No penalties or sanctions apply

# *Monitoring: Compliant (C)*

---

- Requirements are subject to partial CMEP:
  - Spot Checks
  - Self-Report
  - Self-Certification
  - Investigations
  - Periodic Reports
  - Penalties and Sanctions
- Audits may not begin until AC phase

# *Monitoring: Auditably Compliant (AC)*

---

- 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

# *Semi Annual Self Certifications*

---

- All entities in the C and AC phases of the CIP Implementation Plan are required to self certify
- Self certifications will be semi annual for the foreseeable future
  - January 15<sup>th</sup>
  - July 15<sup>th</sup>
- WECC will provide 30-day notice and form preview on portal

# *NERC CMEP Implementation Plan*

---

- NERC establishes CMEP Implementation Plan each year
  - Actively monitored standards
  - Frequency and type of monitoring process
- All Regions will be spot checking all 13 requirements for all Table 1 entities in the AC phase between 7/1/09 and 12/31/10
  - Most Regions will attempt to complete all Table 1 spot checks by 7/1/10...

# *CIP Spot Check and Audit Plan*

---

- “Table 1” spot checks: 31 between 7/1/2009 and 7/1/2010 (29 actual onsite visits)
  - Only 13 requirements are in scope
  - Return to 3 year cycle after spot check “wave”
- “Table 2” audits: 26 beginning 7/1/2010
  - 41 requirements in scope
  - Every 3 years for BA/TOP
- “Table 3” audits: 45 beginning 1/1/2011
  - 41 requirements in scope
  - Every 6 years for all other applicable functions

# *Spot Check Scope: 7/1/09*

---

- 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
- Any other CIP standard at the “C” phase where warranted

# *Spot-Checks vs. Audits*

---

- Some minor differences...
  - The report
  - Advance notice (20 vs. 60)
  - No limit on # of standards in spot check
  - Not an investigation
  - Virtually interchangeable terms
- Most everything else will feel just like a compliance audit

# *CIP RSAWs*

---

- New improved RSAWs recently received from NERC; should be public soon
- CCWG responded with comments to First 13 requirements
  - Two day initial review and comment window
  - Will respond with full comment set from CCWG by May 30<sup>th</sup>
- Will use *current* RSAWs for 60-day notice

# *CCWG Spot Check Approach*

---

- CIP Compliance Working Group consistent approach
- Agreed upon by all Regions
- High degree of alignment between all programs; very slight deviations
- CCWG communicates with Regional Managers (RCIG/CMPWG) and NERC on approach elements

# *Pre Spot Check Details*

---

- Though not required, WECC will provide a 60-day notice
- Notice will look very similar to the standard compliance audit notice
- Electronic Data Submittal for non-sensitive information will be required (portal)
- Pre spot check review of non-sensitive information will be done offsite

# *Electronic Data Submittals*

---

- HTTPS connection to Portal
- Should you need additional encryption, please use PGP/GPG
  - WECC will be providing our public key on the portal in the next few days
  - Please upload yours through the portal
- No “symmetric” encrypted packages will be allowed in the future

# *Sidebar: Sensitive Information*

---

- FERC Order 672, 672-A
- 18CFR39.2
- NERC Rules of Procedure, S1500
- NERC CMEP
- WECC CMEP
- No entity-specific NDAs will be signed
- *Doing everything possible to minimize or eliminate the need to take any sensitive information offsite*

# *Preparing For The Spot Check*

---

- All documentation must be electronic
- Where PDFs are used, please scan with Optical Character Recognition (OCR) enabled – no image PDFs unless there is no other option
- All other standard formats are acceptable
- Highlighting and embedded comments can be used to identify specific points of reference

# *Preparing For The Spot Check*

---

- CD/DVD-ROM or USB is satisfactory
- One folder per standard, with subfolders for each requirement:
  - Overview documentation w/ hash tables
  - QRSAW, completed
  - All supporting evidence (repeat/copies)
  - Copies of self reported violations
  - Copies of active mitigation plans and current milestone status

# *Preparing For The Spot Check*

---

- Provide SHA-256 hash records for each document submitted as evidence
- Any SHA-256 hash tool can be used
- Any document with an inconsistent hash or without a hash will need to be re-submitted with respective hash
- Hash values will be verified before acceptance into the record

# *Preparing For The Spot Check*

---

- Pre spot check conference call/webex
- Attendees:
  - Lead auditor
  - Most if not all of the audit team
  - Entity
- Will go over all preparation issues, last minute details and logistics

# *The Onsite Visit*

---

- Small CIP-specific teams of 4+ persons
  - May or may not be separate from Reliability Standard audits
- A WECC employee will lead audit
- Will probably contain a NERC and/or FERC staffer
- Will need your CIP subject matter experts available for interviews, questions and supporting documentation

# *The Onsite Visit*

---

- WECC will arrive [most often] by 1:00PM
- WECC will give opening presentation, roughly 30 minutes or less
- Entity will give opening presentation, roughly 30 minutes or less
- Spot check or audit will commence
- Will need a conference room that can hold up to 10 people

# *The Onsite Visit*

---

- Interviews and Data Requests will be uniquely tracked
- Requests will come as emails to Compliance Contacts
- Interviews will be:
  - Reviewed; summary will need to be approved and attested by the Compliance Contact
  - Attestation and summary notes will be hashed and entered as evidence

# *The Onsite Visit*

---

- Using the “jumpkit” model to contain all audit activity and information
  - Server
  - Networking elements, wireless internet
  - Printer/scanner/copier
  - Virtual machines for each auditor
  - Projector
  - Spare parts

# *The Onsite Visit*

---

- Jumpkit (continued)...
  - Auditors will log in to unique virtual machines
  - Web-based audit application manages and tracks all audit activities
  - Completed RSAWs and other audit artifacts are synchronized with master database (portal)
  - Hard drive(s) in server are encrypted (AES)
  - Tunnel to master database is encrypted (SSH)

# *The Onsite Visit*

---

- Jumpkit (continued)...
  - During the audit all evidence media will remain in the room
  - If you require special handling procedures, please be prepared to collect the media at the end of each day and provide it again the following day
  - The jumpkit will remain with WECC at all times

# *The Onsite Visit*

---

- Jumpkit (continued)...
  - At close of audit, all data will be uploaded to master database and all virtual machines “scrubbed” using 7-pass erasing technique (US DOD 5220.22-M 8-306)
  - No information from the audit will be copied to auditor laptops under any circumstances
  - No information from the audit will remain on the jumpkit server at the conclusion of audit

# *The Onsite Visit*

---

- Evidence envelope
  - Tyvek envelope
  - Evidence handling label outside, signed
  - May use evidence bag inside
  - Paper and electronic evidence artifacts
  - Maintained at your facility for duration of audit cycle
  - Must be able to produce envelope immediately upon request

# *The Onsite Visit*

---

- Evidence envelope (continued)...
  - Paper documents:
    - Critical Cyber Asset list - physically signed in ink by your Senior Management Official, as designated in CIP-003.R2 and included in the sealed envelope
    - Certification statement
  - All ROMs/USB tokens submitted as evidence

# *The Onsite Visit*

---

- All data requests are required to be submitted by 2:00PM on the day prior to conclusion (usually Thursday)
- Audit should conclude Friday morning or mid-day
- WECC will give an exit briefing of all possible new violations and suggestions, roughly 30 minutes

# *Post Spot Check Items*

---

- Spot check report should be provided to entity within 4 weeks (one month) – hopefully sooner...
- Entity will get a chance to review and comment on the final report
- If no violations exist, the report does not go to NERC; if so, it does

# *2009-2010 Spot Check Schedule*

---

- Will be posted on the Compliance website
  - Please let us know immediately if you have scheduling concerns and we will try to accommodate if possible...
- 2009: one team, no contractors, spaced
- 2010: two teams, contractors, compressed
- “Incentive” to complete all Table 1 spot checks before 7/1/10

# 2009 Table 1 Spot Checks

---

- DOPD: 7/6 – 7/10
- GCPD: 7/20 – 7/24
- IPCO: 8/3 – 8/7\*
- CCPD: 8/17 – 8/21
- SPP: 9/14 – 9/18\*
- WACM: 9/28 – 10/2\*
- CISO: 10/12 – 10/16\*
- WAUW: 11/2 – 11/6
- WALC: 11/30 – 12/4

\* Part of regularly scheduled compliance audit

# 2010 Table 1 Spot Checks

---

- EPE: 1/4 – 1/8
- TPWR: 1/11 – 1/15
- NPC: 1/25 – 1/29
- PGE: 2/1 – 2/5
- IID: 2/15 – 2/19
- MULTI: 2/22 – 2/26 (3 entities at once)
- PSC: 3/8 – 3/12
- PNM: 3/15 – 3/19
- SCL: 3/29 – 4/2

# 2010 Table 1 Spot Checks

---

- PSE: 4/5 – 4/9
- SRP: 4/12 – 4/16
- NWC: 4/19 – 4/23
- TEP: 5/2 – 5/7
- BPA: 5/10 – 5/14
- SMUD: 5/17 – 5/21
- TID: 5/24 – 5/28
- LADWP: 5/31 – 6/4
- PAC: 6/7 – 6/11
- AVA: 6/14 – 6/18
- APS: 6/21 – 6/25

# *Other Pre AC Spot Checks*

---

- Compliant (C) phase allows for spot-check, per CMEP
- Some entities will be spot checked for CIP-002 and other standards, per their self certification responses and completed mitigation plans
- Would still be audited during “regular” cycle/phase

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

# *Show and Tell*

---

- Tell the auditor how you meet the requirement (protocol)
  - Often policy, process, procedure, etc
- Show the auditor that you are actually meeting the requirement (proof)
  - Often supporting evidence such as logs, spreadsheets, documents, database extracts, captures, etc
- Covering both angles is best

# *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

# *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

# *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, Continued...*

---

- 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 magnification on the microscope
  - Make it obvious, transparent and simple

# *CIP Compliance Tips, Continued...*

---

- 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, Continued...*

---

- 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 – [compliance.wecc.biz](http://compliance.wecc.biz)
  - WECC PSWG – [roger.serra@seattle.gov](mailto:roger.serra@seattle.gov)
  - WECC DEWG – [vkissner@ci.tacoma.wa.us](mailto:vkissner@ci.tacoma.wa.us)
  - WICF – [www.wicf.biz](http://www.wicf.biz)
  - EnergySec – [www.energysec.org](http://www.energysec.org)

# *Regional Consistency*

---

- CIP Auditors from other Regions will participate in WECC spot-checks/audits
- CCWG – CIP Compliance Working Group
  - Compliance specific
- CIPMWG – CIP Managers Working Group
  - Not compliance specific
- [www.RegionalEntities.org](http://www.RegionalEntities.org)
  - CIP-003.R4.1 already posted\*

# *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
- Registered Entities are holding training
  - Not WECC-sponsored, but conduit
  - Get trained by ISACA and IIA

# Questions?

---

**Patrick Miller**  
**Manager, CIP Audits and Investigations**  
Western Electricity Coordinating Council  
7600 NE 41<sup>st</sup> Street, Suite 160  
Vancouver, WA 98662  
pmiller@wecc.biz  
360.567.4056

**Stacy Bresler**  
**Sr. Compliance Engineer, Cyber Security**  
Western Electricity Coordinating Council  
7600 NE 41<sup>st</sup> Street, Suite 160  
Vancouver, WA 98662  
sbresler@wecc.biz  
360.567.4058

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