



Western Electricity Coordinating Council

CIP-003 Workshop

WECC Critical Infrastructure Protection User Group (CIPUG)
Grand Hyatt - Denver, CO
April 14th, 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

- CIP Compliance

- Bill Fletcher – Compliance Engineer, CIP
 - 360.567.4061 | wfletcher@wecc.biz
 - <https://twitter.com/williamfletcher>
- Stacy Bresler – Sr. Compliance Engineer, CIP (4/20)
 - 360.567.4058 | sbresler@wecc.biz
 - <https://twitter.com/stacybre>
- Patrick Miller – Manager, CIP Audits
 - 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!]*
 - Melanie Wood
 - Cathy Bakk

CIPUG Website

The screenshot displays the WECC Compliance website. At the top, the WECC logo is on the left, and navigation links for Compliance Home, WECC Home, Quick Links, Staff Directory, RMS, and Portal Login are on the right. Below the logo, the word "Compliance" is prominently displayed. A horizontal menu contains links for Entity Registration, Reliability Standards, Compliance Library, Audits & Investigations, Enforcement, and Outreach. The Outreach link is highlighted with a red arrow. On the left side, a vertical navigation menu lists various sections, with "Critical Infrastructure Protection User Group (CIPUG)" selected and highlighted in blue. A red arrow with the number "2" points to this menu item. The main content area shows the "Outreach Home" page, which includes a paragraph about WECC's Outreach Plan and a list of links such as "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".

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

0

CIPUG Outreach

- CIP-004, May 6th, Albuquerque
 - CIP Open Mic(s), June **TBD**
 - CIPUG/ESEC Summit, Summer, Seattle
 - Ongoing CUG meeting participation
-
- *To join the CIPUG email distribution list, send subscribe request to: linda@wecc.biz*

WECC CIPUG Workshops

- #1 request was for examples
 - WECC Compliance can't do that, but *you* can
- 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**

Industry Expert Panelists

- Steve Hamburg
 - James Mapes
 - Wes Miller
 - Jasvir Gill
-
- Please feel free to approach them directly during breaks, lunch and after the event

Asset Owner Presenters

- Ernie Hayden, Seattle City Light
- Lisa James, Chelan County PUD

- Please thank them for volunteering for this event!

CIP-003 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

CIP-003 Key Definitions

- **Policy:** A High level overall plan embracing the general goals and acceptable procedures specially of a government body¹
- **Process:** A series of actions or operations leading to a specific result²
- **Procedure (Operating):**
A document that identifies specific steps or tasks that should be taken by one or more specific operating positions to achieve specific operating goal(s). The steps in an Operating Procedure should be followed in the order in which they are presented, and should be performed by the position(s) identified.³

¹ <http://www.merriam-webster.com/dictionary/policy> (2b)

² <http://www.merriam-webster.com/dictionary/process> (2b)

³ <http://www.nerc.com/page.php?cid=2%7C20%7C283>

CIP-003 Inclusion

- CIP-005.R1.5 – Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter...
 - CIP-003 **all requirements**
- CIP-006.R1.8 – Cyber Assets used in the access control and monitoring of the Physical Security Perimeter
 - CIP-003 **all requirements**

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-003 Evidence

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

CIP-003 Requirement 1

- *CIP-003.R1: Cyber Security Policy – The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following...*
- *AC on 7/1/2009; Table 1*

CIP-003.R1.1 Evidence

- *The Cyber Security Policy must reference the requirements in CIP-002 – CIP-009*
- The cyber security policy can be part of a larger corporate policy providing that the overall policy demonstrates management's commitment to addressing the requirements of these CIP standards and provides a framework for the governance of these standards

CIP-003.R1.1 Evidence

- *The Cyber Security Policy must contain a provision for emergency situations*
- Commonly evidenced by respective policy language with an associated process or method to determine:
 - What is an emergency?
 - Who can declare an emergency?
 - When the emergency begins and ends?

CIP-003.R1.2 Evidence

- *The Cyber Security policy is available to all personnel who have access or are responsible for Critical Cyber Assets*
- Commonly evidenced by:
 - URL and screenshot of corporate intranet site
 - Copies of print material used where electronic access is unavailable
 - Policy statements referencing availability of the policy

CIP-003.R1.3 Evidence

- *The cyber security policy is reviewed and approved annually by the senior manager identified in CIP-003.R2*
- Commonly evidenced by:
 - Review schedule, both historical and future
 - Signed [approved] policy versions and associated timestamps

CIP-003.R1 Evidence Summary

- Modify existing, or create new policy language to reference and require adherence to the CIP Standards
- Understand and document what constitutes an emergency circumstance for your organization
- Demonstrate 100% availability of the policy to all appropriate personnel
- Document annual policy approvals

CIP-003 Requirement 2

- *CIP-003.R2: Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009*
- *AC on 7/1/2009; Table 1*

CIP-003.R2.1 Evidence

- *The senior manager shall be identified by name, title, business phone number, business address, date of designation*
- Commonly evidence by a formal business document capturing all above details

CIP-003.R2.2 Evidence

- *Changes to the senior manager must be documented within thirty calendar days of the effective date*
- Commonly evidenced within the same formal business document from CIP-003.R2.1 to maintain history and continuity

CIP-003.R2.3 Evidence

- *The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy*
- Commonly evidenced by:
 - Respective policy statement
 - Actual approval statement or signature within exception documentation

CIP-003.R2 Evidence Summary

- Formal business documentation to record the responsible senior management official, including all necessary details
- Maintain document history and capture all modifications within appropriate timeframe
- Use policy language to establish appropriate governance of the exception process
- Exception process documentation

CIP-003 Requirement 3

- *CIP-003.R3: Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s)*
- *AC on 7/1/2009; Table 1*

CIP-003.R3.1 Evidence

- *Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s)*
- Commonly evidenced within formal exception documentations

CIP-003.R3.2 Evidence

- *Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk*
- Commonly evidenced within formal exception documentation

CIP-003.R3.3 Evidence

- *Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.*
- Commonly evidenced within formal exception documentation

CIP-003.R3 Evidence Summary

- An exception process should have at least four steps:
 - Identification - identification of the potential exception to a policy
 - Documentation - documentation of the exception within a formal document that captures all necessary information to meet R3
 - Initial review - review and approval or denial of the exception by the entity's senior manager or delegate
 - Annual review - a documented review and approval of any exceptions by the entity's senior manager or delegate
- Any exception documents must include:
 - The policy for the exception being requested
 - An explanation of why the policy can not be met
 - Compensating measures in place to minimize the impact of the exception or a statement accepting risk

Monitoring: Pre-Compliant (BW, SC)

- Subject to partial CMEP:
 - Self-Certification
- Semi-annual Self Certifications
 - July 15th & January 15th
 - Will continue until past AC phase
- Audits may not begin until AC phase
- No Self Reports or Mitigation Plans are due during these phases
- No penalties or sanctions

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

CIP RSAWs

- Just received new and improved draft RSAWs for review from NERC
 - Deadline for comments is 4/17
 - No CIP-002 through 009 RSAWs included
 - Not being distributed to the general industry for comment; only Regional distribution

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 **upfront**
- Again, be mindful of sensitive information

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

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

*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”

* 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 Target Dates

- Ballot Round One*
 - April 1st through April 10th
 - Closed at 8PM on April 10th
 - At least one negative vote and comments were expected – and received – which prompted round two...

*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

43 ** 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
 - Other substantive changes

CIP Violation Severity Levels (VSLs)

- Current CSO706 Drafting Team has issued the VSLs for CIP-002 through 009 V1 and V2 for comment*
 - Plus VRFs for V2 – CIP-003 through 009
 - Comment period open until April 20th
 - Depending on the number of comments, may or may not be adopted prior to July 1st 2009

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
 - 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
- No Registered Entity training – yet...
 - Use the RSAWs and Yellow Book
 - Get trained by ISACA and IIA

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

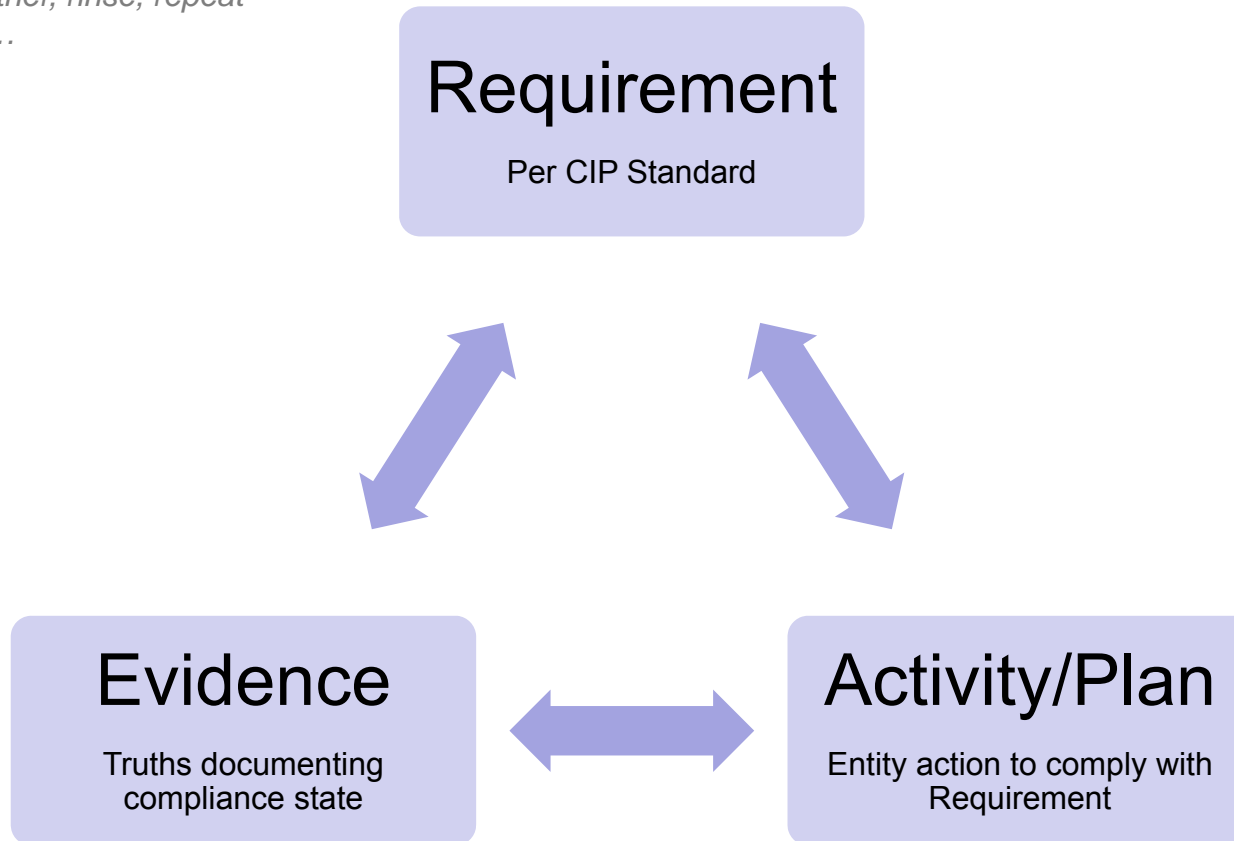
- Change the way you do business
 - Don't just patch together existing documents
 - Demonstrate a true shift toward a more secure posture

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
 - WECC PSWG – roger.serra@seattle.gov
 - WECC DEWG – vkissner@ci.tacoma.wa.us
 - WICF – www.wicf.biz
 - EnergySec – www.energysec.org

Perpetual Compliance Cycle

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



Questions?

Patrick Miller CISA, CISSP-ISSAP
Manager, CIP Audits and Investigations
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