



Western Electricity Coordinating Council

CIP-004 Workshop

WECC Critical Infrastructure Protection User Group (CIPUG)
Marriott Albuquerque - Albuquerque, NM
May 6th, 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.

WECC CIPUG Workshops

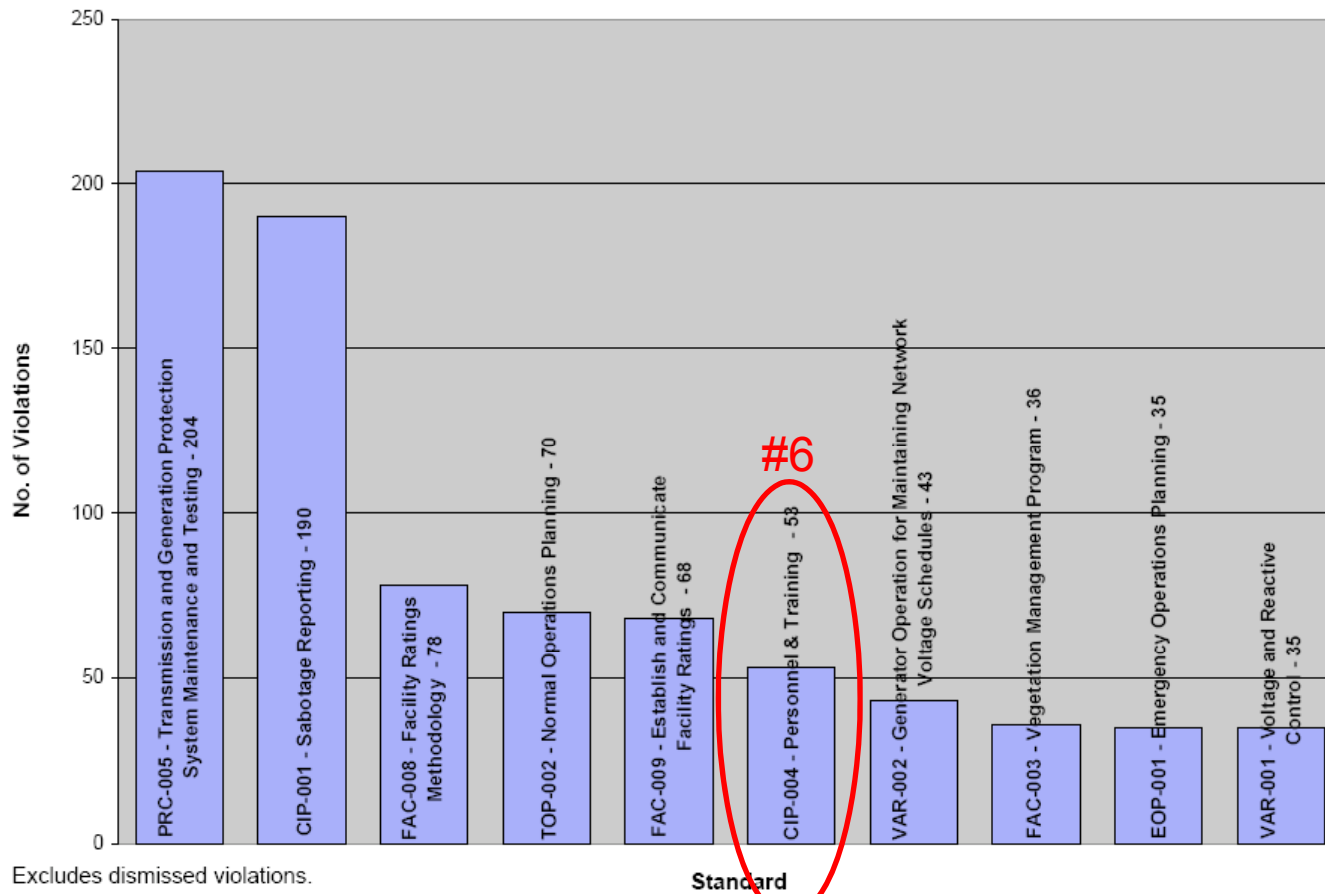
- #1 request was for examples
 - WECC audit can't do that, but *you* can
- New CIPUG workshop model...
 - Asset owner volunteer panel walks through their organization's implementation
 - Industry expert panel of consultants and vendors provides feedback
 - Audience participation is strongly encouraged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

WECC CIP Statistics

- Self Reported Violations*: 173/31 (204)
- Mitigation Plans in Progress: 14
- Completed Mitigation Plans: 171
- Entities with Critical Assets: 326 (of 374)
- Entities with Critical Cyber Assets: 63
- Most Violated Standard: CIP-004
- Most Violated Requirement: CIP-004.R2

2008 NERC CIP Statistics

Top 10 FERC Enforceable Standards
(Submit Dates: 1/1/2008 thru 12/31/2008)



Excludes dismissed violations.

Report Date: 1/5/2009

CIP-004 Purpose

- CIP-004-1.A.3

- Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness...

Industry Expert Panelists

- Bill Addington
 - Bryan Geraldo
 - Steve Hamburg
 - Edward Vasko
 - John Waters
- Please feel free to approach them directly during breaks, lunch and after the event

Asset Owner Presenters

- Joel Brilliant, Sempra Energy
- Mary Robinson, Puget Sound Energy
- Richard Salvo, NV Energy

- Please thank them for volunteering for this event!

CIP-004 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-004 Inclusion

- CIP-005.R1.5 – Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter...
 - CIP-004.R3
- CIP-006.R1.8 – Cyber Assets used in the access control and monitoring of the Physical Security Perimeter
 - CIP-004.R3

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-004 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-004 Requirement 2

- *CIP-004.R2: Training – The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary*

CIP-004.R2 Evidence

- Commonly evidenced by a formal document outlining:
 - The cyber security training program
 - To whom it applies (e.g. unescorted)
 - Delivery, review and update frequencies

CIP-004.R2.1 Evidence

- *This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization*
- Commonly evidenced by training [attendance] logs
 - For all respective personnel
 - Contain date of authorization **and** date of training
 - Can be extract from database or sign-in sheet

CIP-004.R2.2 Evidence

- *R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:*
 - *R2.2.1. The proper use of Critical Cyber Assets;*
 - *R2.2.2. Physical and electronic access controls to Critical Cyber Assets;*
 - *R2.2.3. The proper handling of Critical Cyber Asset information;*
 - *R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident*
- Commonly evidenced through provision of the actual training material

CIP-004.R2.3 Evidence

- *The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records*
- Commonly evidenced by:
 - Training [attendance] logs
 - Supporting policy language requiring annual training

CIP-004 Requirement 3

- *CIP-004.R3: Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:*

CIP-004.R3 Evidence

- Commonly evidenced by:
 - A formal document outlining
 - The personnel risk assessment program
 - To whom it applies and why
 - Records indicating when the PRA was conducted including when the person was granted access (to verify 30-day window)

CIP-004.R3.1 Evidence

- *The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.*
- Commonly evidenced as...
 - Elements within the formal Personnel Risk Assessment program documentation
 - HR or third party database/application/spreadsheet view with proof of assessment
 - Cover page of assessment results

CIP-004.R3.2 Evidence

- *The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.*
- Commonly evidenced by...
 - Policy or PRA program language
 - Criteria with respect to “for cause”
 - Schedules for re-assessment

CIP-004.R3.3 Evidence

- *The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.*
- Commonly evidenced by...
 - HR or third party database/application/spreadsheet view with proof of assessment matched against CIP-004.R4 list
 - Contract agreements and associated documentation
 - Cover page of assessment results

CIP-004 Requirement 4

- *CIP-004.R4: Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.*
- Commonly evidence by a spreadsheet, database or other application that can track all respective access

CIP-004.R4.1 Evidence

- *The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.*
- Commonly evidenced by...
 - Policy or program language
 - Contract agreements or associated documentation
 - Update frequency records

CIP-004.R4.2 Evidence

- *The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.*
- Commonly evidenced by...
 - Policy or program language
 - Revocation records

CIP-004 Compliance Tips

- Adopt what works already!
 - Safety program? Usually one of the most mature programs.
 - Leverage your communication department if you have one.
- Look for opportunities to link compliance evidence.
 - For example, your personnel risk assessment evidence mapped to physical access evidence mapped to electronic access evidence mapped to training evidence.
 - Each piece of evidence by itself may look OK...coupled together may present a different picture..

CIP-004 Compliance Tips

- R.1 / Awareness

- Design a program you can live with! (and meets the detailed requirements)
- Don't forget it's quarterly!

- R.2 / Training

- No one said it had to be a PowerPoint presentation.
- Design your program to best suit your organizations culture.

CIP-004 Compliance Tips

- R.3 / Personnel Risk Assessment

- Don't miss this: (R.3.3) "...shall document the results of personnel risk assessments of its personnel having **authorized cyber or unescorted physical access** to Critical Cyber Assets..."

- R.4 / Access

- Back to the general statements. Map it all together so the whole picture can be seen.
- Specific electronic and physical access rights to Critical Cyber Assets matter.
 - User provisioning /de-provisioning systems can help greatly

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

*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

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

CIPS v2 Target Dates

- Ballot Round One
 - At least one no vote or comment was received, so second ballot was issued
- Ballot Round Two
 - Closed on 4/27
 - Approved
- Should be at the next BOT meeting for vote

*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

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

CIP v3

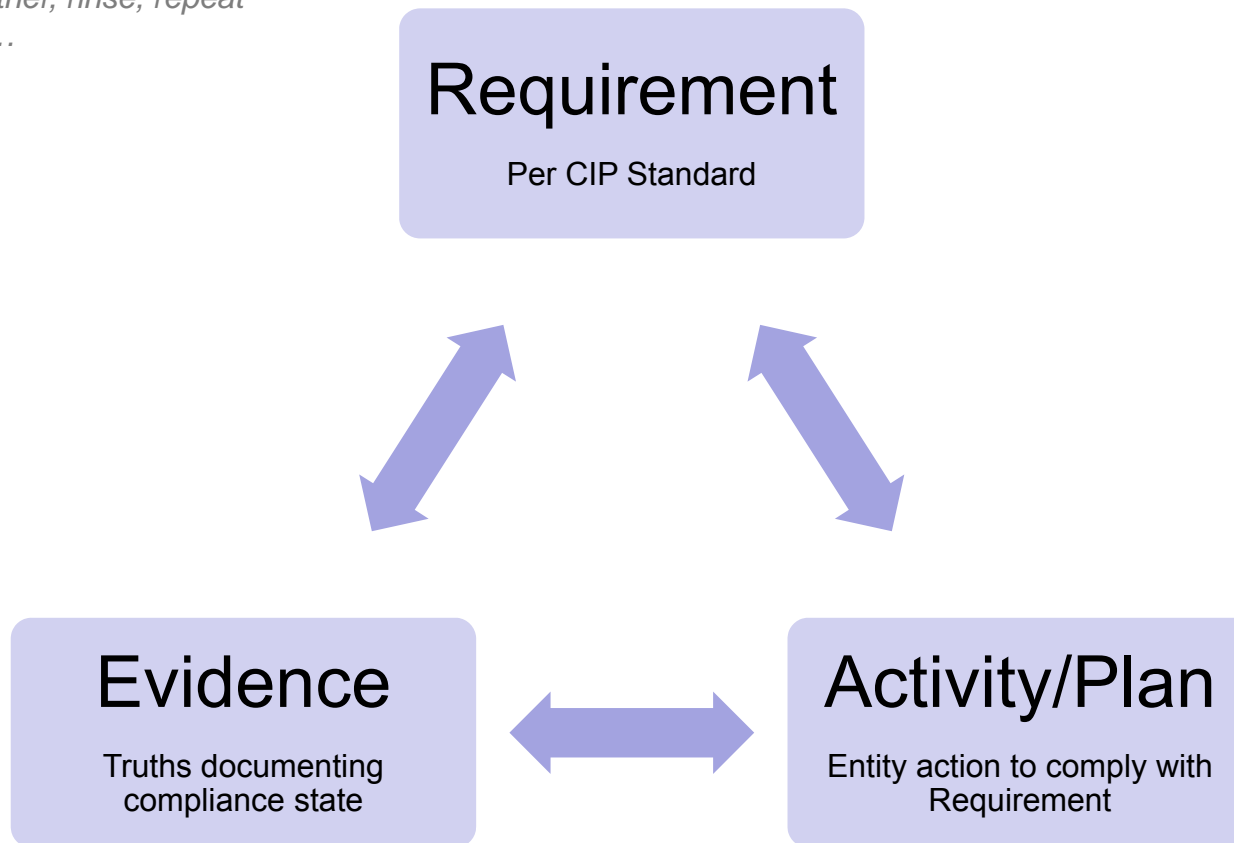
- Drafting team from v2 is already chartered (per SAR) to begin drafting v3
- Early discussions include:
 - Serial and other protocols
 - Encryption
 - Forensics
 - Alignment with NIST
 - Other substantive changes

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

Perpetual Compliance Cycle

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



Questions?

Patrick Miller
Manager, CIP Audits and Investigations
Western Electricity Coordinating Council
7600 NE 41st 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 41st Street, Suite 160
Vancouver, WA 98662
sbresler@wecc.biz
360.567.4058

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