



Western Electricity Coordinating Council

CIP Compliance Update

WECC Critical Infrastructure Protection User
Group (CIPUG)

Doubletree Lloyd Center, Portland, OR
February 23, 2010

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 CIP Statistics

- Entities with Critical Assets: 79
- Entities with Critical Cyber Assets: 58
- CIP-Applicable Entities: 333 (of 462 total Registered Entities in WECC)

WECC CIP Statistics

- Total violations reported: 154
- Total violations dismissed: 13
- Total enforceable violations: 141
- Total violations fully mitigated: 92
- Total open violations: 49
- Most violated standard: CIP-004
- Most violated requirement: CIP-004.R3

WECC CIP Statistics

Most violated standards:

- CIP-004: 58
- CIP-007: 28
- CIP-003: 17
- CIP-002: 10
- CIP-009: 10

WECC CIP Statistics

Most violated requirements:

- CIP-004.R3: 21
- CIP-004.R2: 19
- CIP-004.R4: 18
- CIP-007.R1: 12
- CIP-003.R1: 7

WECC CIP Spot Check Statistics

- 12 of 29 CIP Spot Checks performed
- An average of 3.6 findings per Spot Check
- Most violated Standard/Requirement on Spot Checks is CIP-004.R3
- Spot Check reports are issued within an average of 82 days
- Average of 93.5% satisfaction, based on feedback forms received

Lessons Learned

- Outreach is worth every penny and more
- CIP information is sensitive, in many ways
- Some outside consultants have helped the entities, some haven't

Lessons Learned

- Strict time management is necessary to complete the Spot Check on time
- Constant, transparent communication with the entity is best
- Efficiencies have been found through summary tables and sampling

Lessons Learned

- Document organization and presentation is not yet mature
 - Revision history w/ specific changes recorded
 - Classification
 - Version numbers
 - Applicable dates
 - Entire audit period
 - Approver, owner, signatures
 - Holistic, formalized, intentional

Lessons Learned

- SMEs are very very smart and they know their work, but they are not auditors
- Responses to entity questions are often highly specific and not generally applicable to all entities

CIP Approach – Security Policy

- Must address the requirements of CIP-002 through CIP-009
 - WECC does a policy map exercise to validate “addresses the requirements...” per R1.1
 - “Company shall adhere to all Federal, State and Local regulations” is too generic
 - Not a *procedure* but a *policy*
 - Does not need to be a single policy document
 - Does not reach down to subrequirement level

CIP Approach – Security Policy

Cyber Security Policy Completeness Comparison					
Version 1.0 / DATE			Version 2.0 / DATE		
T/F	Standard/Requirement	Addressed? (comments)	T/F	Standard/Requirement	Addressed? (comments)
	CIP-002-1.R1			CIP-002-1.R1	
	CIP-002-1.R1.1			CIP-002-1.R1.1	
	CIP-002-1.R1.2			CIP-002-1.R1.2	
	CIP-002-1.R1.2.1			CIP-002-1.R1.2.1	
	CIP-002-1.R1.2.2			CIP-002-1.R1.2.2	
	CIP-002-1.R1.2.3			CIP-002-1.R1.2.3	
	CIP-002-1.R1.2.4			CIP-002-1.R1.2.4	
	CIP-002-1.R1.2.5			CIP-002-1.R1.2.5	
	CIP-002-1.R1.2.6			CIP-002-1.R1.2.6	
	CIP-002-1.R1.2.7			CIP-002-1.R1.2.7	
	CIP-002-1.R2			CIP-002-1.R2	
	CIP-002-1.R3			CIP-002-1.R3	
	CIP-002-1.R3.1			CIP-002-1.R3.1	
	CIP-002-1.R3.2			CIP-002-1.R3.2	
	CIP-002-1.R3.3			CIP-002-1.R3.3	
	CIP-002-1.R4			CIP-002-1.R4	

CIP Approach – Security Policy

- Readily available can be challenging to prove...
 - Intranet?
 - Binders?
 - When was it originally “posted?”

CIP Approach – Personnel

- CIP-004 is the most violated CIP standard
- CCWG whitepaper
 - <http://regionalentities.org/RegionalComplianceImplementationGroup.aspx>
- Evidence of specific access rights, training and personnel risk assessments will be requested for employees, contractors and vendors
 - Do not provide actual results of background checks, only verification and type

CIP Approach - Personnel

- CIP-004 summary table can really help (supporting data is still required):
 - Employee ID and name
 - **Date electronic access granted**
 - **Date physical access granted**
 - Date electronic access removed
 - Date physical access removed
 - Date of original training
 - Date of annual training
 - Date PRA completed

CIP Approach – Security Testing

CIP-007.R1

- **Functional testing vs. security testing**
 - **See the FAQ – CIP-007 Q4, page 23**
 - Basic port scans
 - File integrity checking
 - User account review
 - Access controls, audit functions, etc...
- **Test results vs. performance results**

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)
 - Supporting evidence: logs, spreadsheets, documents, database extracts, captures, etc
- Attestations alone are not sufficient except for “no event” situations

Who & When?

- Table 1 entities will undergo CIP Spot Checks through 12/31/2010
 - First 13 requirements: 1/1/2010 – 6/30/2010
 - All 41 requirements: 7/1/2010 – 12/31/2010
- Table 2 entities will be subject to CIP Compliance Audits of all 41 requirements as part of their regularly scheduled Compliance Audit as of 7/1/2010

Who & When?

- Table 3 entities will be subject to CIP Compliance Audits of all 41 requirements as part of their regularly scheduled Compliance Audit as of 1/1/2011
- Table 4 entities are on their own schedule – see v1 CIP Implementation Plan
- No change to Actively Monitored standards for 2010; all CIPs are included

Who & When?

- BA and TOP functions are on 3 year schedule
 - CIP Compliance Audits will be bundled (or adjacent) to regularly scheduled audit
- All other functions are on 6 year schedule
 - CIP Compliance Audits will be bundled (or adjacent) to regularly scheduled audit
- Only Table 1 entities are subject to mandatory CIP Spot Checks... *so far*

Technical Feasibility Exceptions

- Received a total of 1090 TFE Part A forms
- 52 entities submitted TFEs
- 25,304 total assets were reported

- Higher numbers were expected, based on the two voluntary TFE surveys
- You will notified when and how to submit your TFE Part B details soon...

Technical Feasibility Exceptions

TFEs by Basis (as of 2/11/2010)

- Adverse effect on BES reliability: 19
- Cannot achieve by compliance date: 29
- Not technically possible: 864
- Operationally infeasible: 35
- Precluded by technical limitations: 135
- Unacceptable safety risks: 8

Technical Feasibility Exceptions

TFEs by Estimated Impact (as of 2/11/2010)

- Minimal impact: 1065
- Moderate impact: 18
- Severe impact: 7

Current TFE Scope

- Requirements eligible for TFE Request:
 - CIP-005-1/R2.4
 - CIP-005-1/R2.6
 - CIP-005-1/R3.1
 - CIP-005-1/R3.2
 - *CIP-006-1/R1.1*
 - CIP-007-1/R2.3
 - *CIP-007-1/R3.2*
 - CIP-007-1/R4
 - CIP-007-1/R4.1
 - CIP-007-1/R5.3
 - CIP-007-1/R5.3.1
 - CIP-007-1/R5.3.2
 - CIP-007-1/R5.3.3
 - CIP-007-1/R6.
 - CIP-007-1/R6.3

Technical Feasibility Exceptions

- FERC's recent position...
 - FERC approved process, but expressed concerns; required 90 day response
 - Added CIP-006.R1.1 and CIP-007.R3
 - Questioned usefulness of Class-Based TFEs
 - Compensating measures must be equal or better security
 - Uniform Part A forms across all Regions
 - Concerned about potential abuse

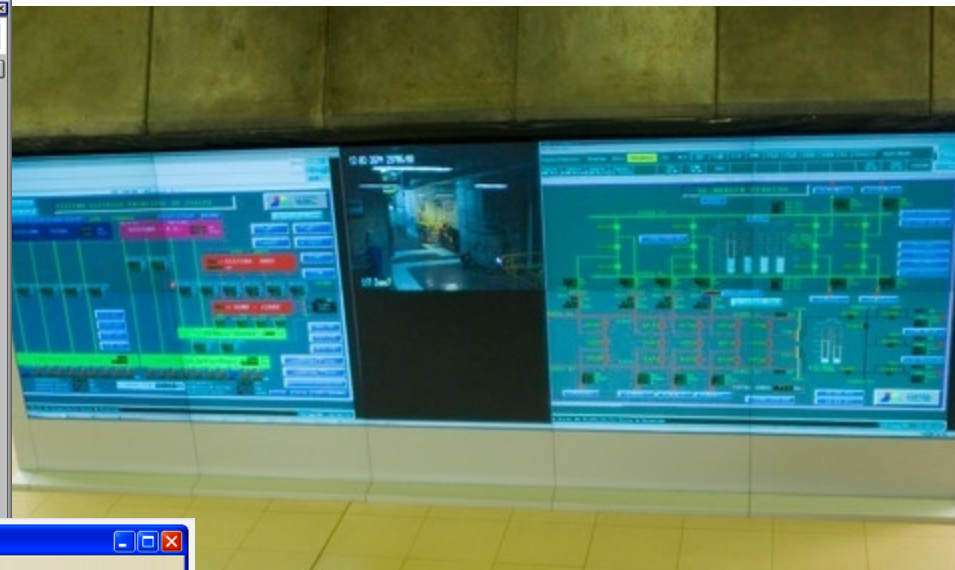
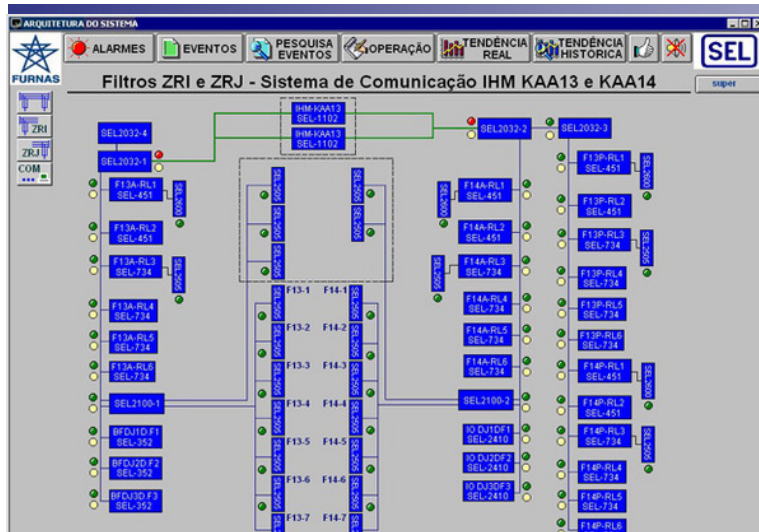
Technical Feasibility Exceptions

- NERC's recent Process Bulletin 2010-001
 - TFEs for CIP-006.R1.1 and CIP-007.R3 submittals between 2/17/2010 and 4/30/2010
 - Portal forms are updated and ready for use

Change Is Good

- Technology and innovation (and threats) will always move faster than regulation
- As more entities apply the standards, more expertise is gained
- After V4, new changes to CIP standards will be small and tactical

Current Events



Mozilla Firefox
http://www.barrow.house.gov/index.php
OBAMA!! Red Eye CREW!!!! O RESTO E HACKER!!! by HADES; m4V3RiCk; T4ph0d4 -- FROM BRASIL

Official web site for Representative John Barrow (D - GA).

29

ONS Operador Nacional do Sistema Elétrico
Login: ok
Senha: Sair
Alterar Senha

Current Events

- SCADA is fertile ground for hacking
 - Uncharted territory; street cred
 - Legacy devices
 - New, untested hardware, software, protocols
 - Smart Meter hacking/worm demonstrations
 - Protocol “fuzzers”
 - SHODAN, cookbooks, Metasploit
 - Supply chain attacks
 - Short story: ***easy target***

Current Events

- China: sophisticated, coordinated, funded
 - Aurora
 - The Google hack, not DPCD INL experiment...
 - Finance and oil industry targets
 - Trojan cameras, USB devices at trade shows
 - Finance, defense and energy industry targets
- APTs (Advance Persistent Threats) and Nation State attacks are real

Current Events

cyberwar - Google Search

Web Images Videos Maps News Shopping Gmail more ▾ pmillerwecc@gmail.com | Settings ▾ | Sign out

Google cyberwar Search Advanced Search

Web Show options... Results 1 - 10 of about 1,140,000 for cyberwar. (0.30 seconds)

[Cyberwarfare - Wikipedia, the free encyclopedia](#)
Jump to [Project of the International Convention on Prohibition of Cyberwar](#): According to this project, **cyberwar** is defined as the use of Internet and ...
[Cyber warrior](#) - [Battlefield](#) - [Tactics](#) - [Reported threats](#)
en.wikipedia.org/wiki/Cyberwarfare - 20 hours ago - [Cached](#) - [Similar](#) - [Print](#) - [Close](#)

[frontline: cyber war!](#) | PBS
The Slammer hit on Super Bowl weekend. Nimda struck one week after 9/11. Code Red had ripped through the system that summer. Moonlight Maze moved into the ...
www.pbs.org/wgbh/pages/frontline/shows/cyberwar/ - [Cached](#) - [Similar](#) - [Print](#) - [Close](#)

[cyberwar](#)
We offer a distinction between what we call netwar--societal-level conflicts waged in part through internetted modes of communications--and **cyberwar** at the ...
www.rand.org/publications/randreview/.../cyberwar.html - [Cached](#) - [Similar](#) - [Print](#) - [Close](#)

[PDF] [CYBERWAR IS COMING!](#)
File Format: PDF/Adobe Acrobat - [Quick View](#)
by J Arquilla - [Cited by 2](#) - [Related articles](#) - [All 21 versions](#)
defining **cyberwar**. Our position is at odds with a view (see Arnett, **cyberwar** principles—they were not called that at the time, of ...
www.rand.org/pubs/monograph_reports/MR880/MR880.ch2.pdf - [Similar](#) - [Print](#) - [Close](#)

News results for **cyberwar**

[Google vs. China: The Tip of the Cyberwar](#) - 4 days ago
Security experts say there's a raging, worldwide **cyberwar** going on behind the scenes, and governments and businesses across the globe need to be on alert. ...
[FOXNews](#) - [11 related articles >](#)
[Cyberwar rekindles arms race](#) - [Sydney Morning Herald](#) - [7 related articles >](#)

[Cyberwar - The U.S. Studies the New Art of Cyberwar - Series ...](#)
Jan 26, 2010 ... The US is developing a strategy to deal with cyberspace attacks, a task complicated by the problem of identifying the enemy.
www.nytimes.com/2010/01/26/world/26cyber.html - 59 minutes ago - [Print](#) - [Close](#)

Sponsored Links
[Cyberwar at Amazon](#)
Millions of titles, new & used.
Qualified orders over \$25 ship free
[Amazon.com/books](#)
[See your ad here >](#)

Current Events

Emerging cyber security Legislative actions...

Emerging Issues	Executive Branch Activity	111 th Congress	110 th Congress	Statutory Framework
National Cybersecurity Strategy	CNCI; 60-Day Review; 2003 NSSC; NMS-CO	S.773; H.R. 4061		44 U.S.C
Executive Branch Organization	Cyber Coordinator; CYBERCOM; DHS NCC, NCSD	H.R. 1174; H.R. 1910; S. 921; H.R. 2165; H.R. 2195; S. 778; 4		44 U.S.C., Sec. 3541-3549
Congressional Oversight Concerns		S. 1494; S. 1438		
Establish/Update Legal Authorities		S. 773; S. 946		
Awareness, Research, Education, Training	DOD Cybercrime Center; DHS NCC	H.R. 2200; H.R. 2454; S. 177; S. 1391; H.R. 2647; H.R. 2892; H.R. 266; H.R. 1		
Outreach, Collaboration and Policy Formation	Cyber Coordinator; DIB Initiative; NIST standards	S. 1436; H.R. 2020; H.R. 1	H.R. 6	

“Fifty federal agencies and 20 congressional committees and subcommittees claim jurisdiction over aspects of federal cybersecurity policy”

Sen. Rockefeller; Chair, Commerce, Science and Transportation Committee; Dec 4 2009

Crystal Ball

- Congressional pressure will continue
 - Expect breach laws to expand this direction
 - Regulation and scrutiny will intensify
 - NERC, FERC and possibly even Regions and asset owners may be called to testify

- FERC will get some additional authority
 - May even include Distribution (Smart Grid)

Crystal Ball

- Agencies are competing for control
 - Some of the new legislation/regulation may not be under DOE or FERC
 - DHS, NSA, NIST (DOC), DOD
- The landscape may shift dramatically if an event is realized
 - TSA is a good example

Crystal Ball

- Arms race between hackers/researchers and product vendors will continue
 - Vendors will always lag
 - Government will use regulation to close gap
 - Utilities are stuck in the middle
- Media spotlight will continue
- Research
 - Universities, McAfee, GreyGoose

Crystal Ball

- CIP standards will continue to evolve
 - Greater degree of prescription and restriction
 - Scope will increase to include more devices
 - More registered functions will be included
- Industry may not maintain the ability to shape security standards going forward unless clear progress is demonstrated

Getting Help

- CUG

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

- CIPUG

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

- EnergySec

- <http://www.energysec.org>

- WICF

- <http://www.wicf.biz>

- NERC

- <http://www.nerc.com>

CIP Audits & Investigations Staff

- Josh Axelrod – Compliance Engineer, Cyber Security
 - 360.567.4067 | jaxelrod@wecc.biz
- Stacy Bresler – Sr. Compliance Engineer, Cyber Security
 - 360.567.4058 | sbresler@wecc.biz
- Brent Castagnetto – Compliance Engineer, Cyber Security
 - 801.597.7957 | bcastagnetto@wecc.biz
- Charles (Chuck) Coulter – Compliance Engineer, Cyber Security
 - 360.567.4062 | ccoulter@wecc.biz
- Bill Fletcher – Compliance Engineer, Cyber Security
 - 360.567.4061 | wfletcher@wecc.biz
- Steven Parker – Sr. Compliance Engineer, Cyber Security
 - 360.567.4055 | sparker@wecc.biz
- John McGhee – Director of Compliance Audits and Investigations
 - 360.567.4060 | jmcghee@wecc.biz

CIP Organizational Changes

- My final day with WECC is March 3rd 2010
- Moving to undisclosed consulting firm
- CIP Team expertise is still there for you
- Spot Checks, Audits remain the same
- No known changes to existing schedule

CIP Organizational Changes

- Special thanks to:
 - WECC management
 - WECC CIP staff
 - WECC Compliance Staff
 - All other WECC staff
 - **WECC registered entities**

- Meet John McGhee
 - Director, Compliance Audits & Investigations

Happy Trails...

- ...until we meet again

millerpatrick.c@gmail.com

503.406.8887

Questions?

