



Western Electricity Coordinating Council

WECC CIPUG Auditable Compliance Workshop

WECC CIPUG Meeting
Salt Lake City Center, Salt Lake City, UT
February 10-11, 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.

Introduction

- Thanks for coming!
- 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 Outreach

- **J. Taud Olsen**

- *Director, Stakeholder Relations and Compliance Outreach*
- Office: 801.582.0353
- Direct: 801.819.7603
- Mobile: 801.883.6894
- tolsen@wecc.biz

- *Thanks to Becky, Kirha and Bobbie for the logistical support!*

CIP Audit Staff

- **Bill Fletcher**

- wfletcher@wecc.biz
- 360.567.4061 (desk)
- 541.912.3226 (mobile)

- **Patrick Miller**

- pmiller@wecc.biz
- 360.567.4056 (desk)
- 503.260.6472 (mobile)

CIP Outreach Calendar

- CIP-008/009, March 18th, Boise
- CIP-003, April 14th, Denver
- CIP-004, May TBD
- CIP Open Mic(s), June TBD
- NERC CIP Standards Development Process, Webex, TBD
- CIPUG/ESEC Summit, Summer, Seattle

Workshop Overview

Day One

- CIP-002 Panel Discussion
- Risk-Based Assessment
- CIP-002 AC Evidence
- CIP-003 AC Evidence
- Q&A

*Not strictly limited to the “First 13”
– any relevant CIPS subject
matter is open for discussion*

Day Two

- CIP-004 AC Evidence
- CIP-007 AC Evidence
- CIP-008 AC Evidence
- CIP-009 AC Evidence
- 2009 CIP Spot-Check and Audit Plan
- CIP Horizon
- Q&A

AC (First 13) 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

Note that CIP-005 and CIP-006 are not in the “First 13” 7/1/09 AC Scope and CIP-001 is already required as part of FERC Order 693



Western Electricity Coordinating Council

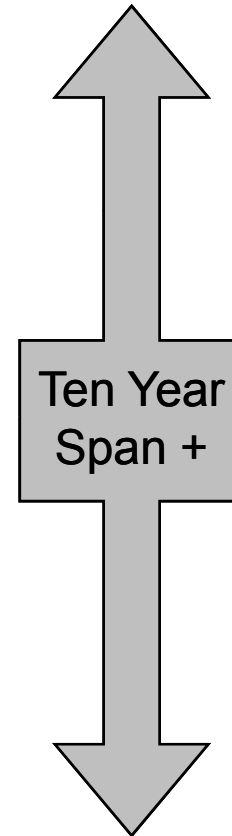
CIP-002 Panel Discussion

*It's 11:59PM. Do you know where your
Critical Assets are?*

CIPS Past to Present

- PDD 63
- FERC SMD Appendix G
- NERC UAS-1200
- NERC 1300
- NERC CIP 002-009
- FERC Order 693 (CIP-001)
- FERC Staff Assessment
- FERC CIPS NOPR
- FERC Order 706
- FERC Order 706-A
- CSO706SDT

...**05/1998**

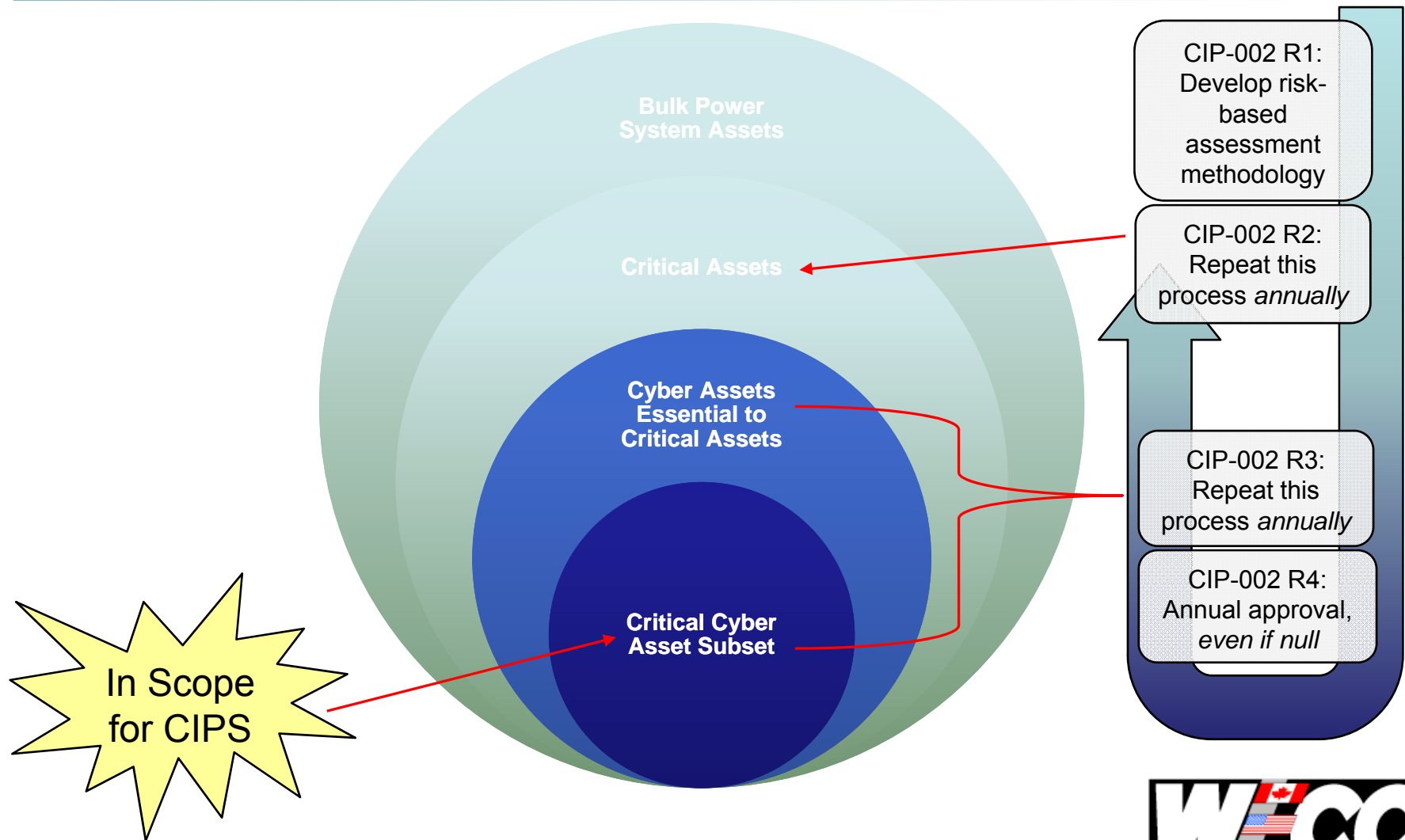


...**02/2009**

CIPS Distilled

- Critical Infrastructure Protection Standards (CIPS) are intended to protect the following:
 - Bulk Power System (Bulk Electric System)
 - Critical Assets, which could be...
 - Control Centers, Transmission Subs, Generation Plants
 - Critical Cyber Assets, which could be...
 - EMS, DCS, RTUs, IEDs, PLCs, Relays
 - Network elements supporting any or all of the above
 - Decision Support Systems
 - Critical Infrastructure Information
- Provide greater reliability through greater security and accountability
 - Who did what, and when...

The CIPS Kernel



What Happens If I Don't?

- \$1M per day, per violation – plus...
- Violation Severity Levels (VSLs)
- Violation Risk Factors (VRFs)
- Mitigating factors
 - Reduce penalties and sanctions
- Aggravating factors
 - Increase penalties and sanctions
 - Any single aggravating factor denies application of any/all mitigating factors
- Can potentially impact perception
 - Rate cases, re-licensing, shareholders, board, customers, etc

CIP Panel Discussion

- Asset Owners
 - Bob Case, Black Hills Corporation
 - Brian McKay, Xcel Energy
 - Please thank them for volunteering
- Industry Experts
 - Steve Fisher
 - Mark Simon
 - Please feel free to approach them during breaks, lunch, and after the event



Western Electricity Coordinating Council

Risk-Based Assessment

NERC BES Definition

From the NERC Glossary of Terms

- Bulk Electric System - As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

FERC BPS Definition

“Bulk Power System” from the EPAct2005

- “SEC. 215. ELECTRIC RELIABILITY.
 - “(a) DEFINITIONS.— For purposes of this section:
 - “(1) The term ‘bulk-power system’ means —
 - “(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and
 - “(B) electric energy from generation facilities needed to maintain transmission system reliability
 - The term does not include facilities used in the local distribution of electric energy

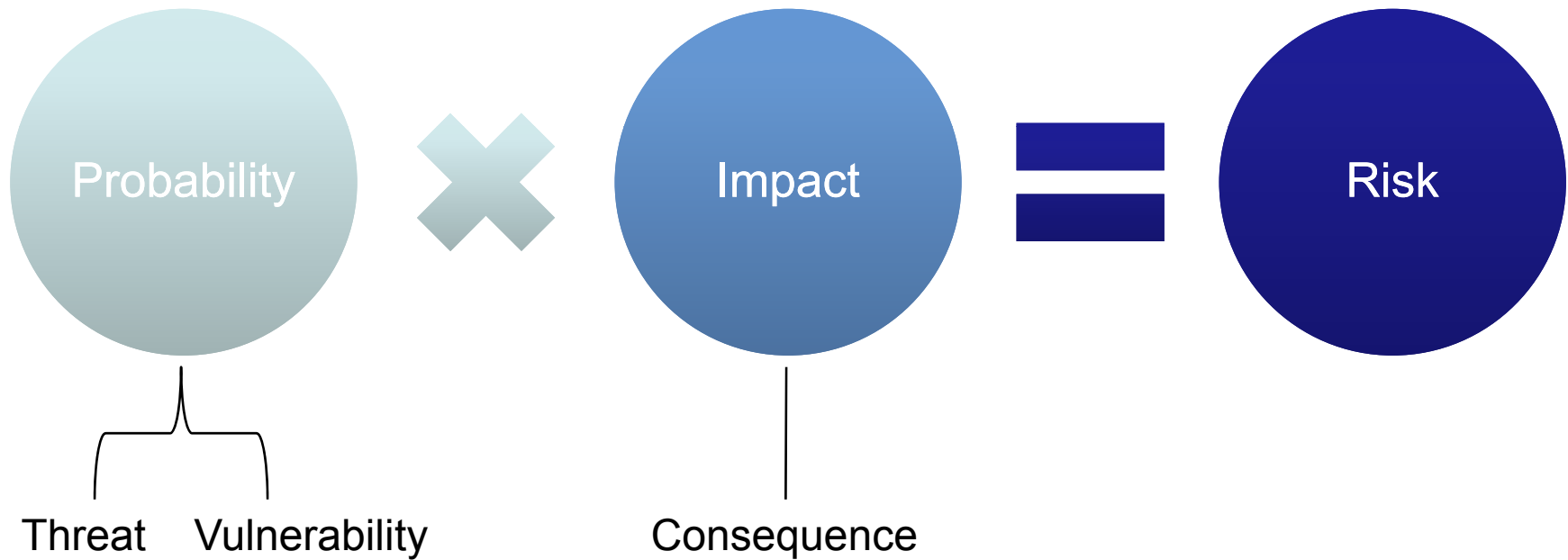
BES vs. BPS

- NERC = BES; FERC = BPS
- Specific exclusion per FERC for Distribution
- ***For the purposes of your RBAM , they are essentially interchangeable***

Simplified Risk Model

- **Risk** = Impact x Probability
- **Impact** = Consequences
- **Probability** = Threat x Vulnerability
 - **Threat** = potential for a particular threat-source to successfully exploit a particular vulnerability
 - **Vulnerability** = a weakness that can be accidentally triggered or intentionally exploited

Simplified Risk Model



Simplified Risk Table

		Probability		
		High	Medium	Low
Impact	High	Red	Orange	Yellow
	Medium	Orange	Yellow	Green
	Low	Yellow	Green	Purple

Most business decisions focus here...

Most *successful* attackers focus here...

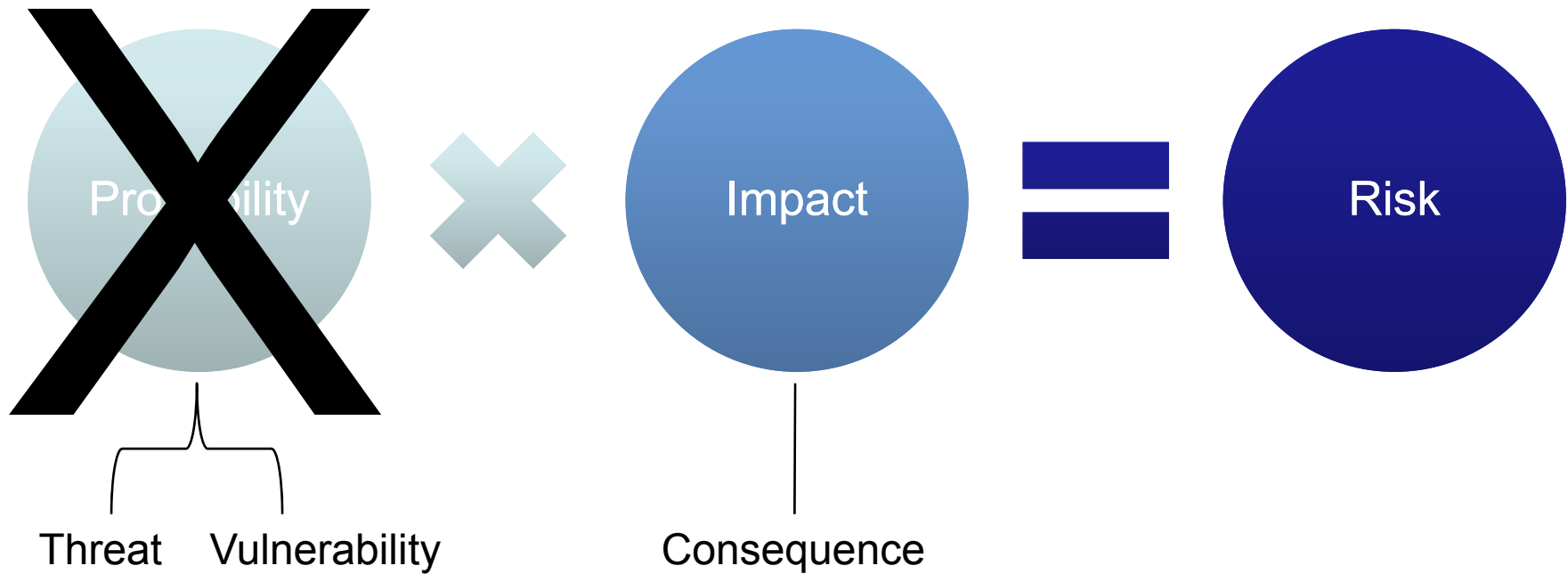
Some Security Perspective

- Weakest link, sure... but where is it?
- Extremely sophisticated modeling systems are available, some very cheap
- New critical vulnerabilities are being discovered on a daily basis
- Most vendors are unresponsive
- Legacy systems are everywhere
- Packets don't care about distance, location or the size of your organization

Risk-Based = Impact

- Throw out the traditional Risk variables
- Set probability to 100% or 1.0
 - Assume the threat exists
 - Assume vulnerability exists
 - Ignore probability
- New result: Risk = Impact x Probability
- ***Risk-based assessment translates into an impact assessment***

Risk-Based Approach



Risk...



The “Simple” Questions

- Does an asset if destroyed, degraded, compromised* or otherwise rendered unavailable, impact the reliability of the Bulk Electric System?
- * What if...
 - The asset were used against the BES?
 - The system(s) were used against the asset?
 - The system(s) were used against neighbors?

NERC RBAM Guidance

- Per FERC Order 706
- Risk Assessment Working Group
 - V1 = Critical Asset ID Guideline*
 - V2 – Critical Cyber Asset ID Guideline
 - Not public yet
 - Sidetracked temporarily while the RAWG responds to comments on V1
- Highly collaborative effort
- Highly effective guideline

* http://www.nerc.com/docs/cip/sgwg/Critical_Asset_ID_V0_8_R0_08262008-Clean.doc

The WECC RBAM

- RBAM = Risk-Based Assessment Methodology
- Geared toward small-to-mid sized entities
- In response to FERC Order 706
- May or may not come from Compliance
 - Feedback loop...
- Should be ready for prime time around mid-March 09

WECC RBAM Guidance

- Scope and applicability language
- General clarification around the use of probability
- Set of guiding principles for consistent identification of Critical Assets within the Region for small-to-mid sized entities
- **Note that it will be provided only as guidance and not a requirement**

WECC RBAM Guidance

- Exhibits/examples under consideration:
 - Compact Criteria Model
 - NERC Guidance
 - FERC Guidance
 - Letters of Negative Assertion
- Expected references:
 - WECC operational documentation
 - NPCC RBAM Guidance
 - OCTAVE Allegro

Quantitative vs. Qualitative

- Quantitative
 - Slower, more expensive, greater depth
 - Easier to justify, support is often pre-defined
- Qualitative
 - Faster, less expensive, greater breadth
 - Not as easy to justify, needs greater support
- Both work and often end up with nearly the same result



Western Electricity Coordinating Council

Evidence Sidebar

CIP Evidence 101 – Do

- Evidence Dos:
 - Connect the dots in advance; try on audit 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 Evidence Types

- What type of evidence is best?
 - Yes. Yes it is. No, really...
 - Word, Visio, Excel, PDF
 - System/event logs
 - Database reports
 - Video, voice or packet captures
 - Floor plans
 - Observations
 - The entity is responsible for proving compliance, so it could be pretty much anything...

Evidence Slide Format

- *Paraphrase/language of CIP standard will be in dark red italics*
- Commonly exhibited evidence below:
 - Often a list will be necessary
 - To present multiple items

What Is Common Evidence?

- Practices that have been commonly demonstrated...
 - Through existing compliance monitoring activities to date
 - Through pre-compliance discussions
 - In other regulatory compliance regimes
- **Note that you are not restricted to the “common evidence” provided herein**



Western Electricity Coordinating Council

CIP-002 AC Evidence

CIP-002 Requirement 1

- *CIP-002.R1: Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.*

CIP-002 R1.1 Evidence

- *The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria*
- Commonly evidenced by:
 - Formal document or set of documents containing the methodology details
 - Meeting minutes
 - Engineering studies

CIP-002.R1.2 Evidence

- The risk-based assessment should consider the following assets:
 - Control centers and backup control centers performing the functions of the entities listed in the Applicability section
 - Transmission substations...
 - Generation resources...
 - Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration
 - Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more
 - Special Protection Systems...
 - Any additional assets...

Must Have A Documented RBAM

- No matter which approach you use, you must have a documented risk-based assessment methodology
 - Quantitative methods usually come with ample supporting documentation
 - Qualitative methods usually need more supporting documentation
- Needs to be a repeatable process for consistency

RBAM Challenges

- Probability doesn't count
- Redundancy doesn't count
 - N-1 can't be sole basis for criticality
- Cost, resources, convenience don't count
- Risk to the asset vs. risk to the BES
- Engineering studies based on agenda
- Operational experience
- Communication with interconnections
- “Dispatchable” and black-start

CIP-002 Requirement 2

- *CIP-002.R2: Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.*

CIP-002.R2 Evidence

- Commonly evidenced by:
 - Any formal document containing said list with all appropriate details; **even if the list is null**
 - Supporting lists used during evaluation such as list of all assets in scope for consideration
 - Engineering studies
 - Annual review meeting minutes
 - Entity Subject Matter Experts (SMEs)

CIP-002 Requirement 3

- *CIP-002.R3: Critical Cyber Asset Identification — **Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:***
 - *R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
 - *R3.2. The Cyber Asset uses a routable protocol within a control center; or,*
 - *R3.3. The Cyber Asset is dial-up accessible*

** Emphasis added*

CIP-002.R3 Evidence

- Commonly evidenced by:
 - Any formal document containing said list with all appropriate details; **including null lists**
 - Supporting lists used during evaluation such as list of all cyber assets in scope for consideration
 - Supporting lists of protocols and other communication options considered
 - Annual review meeting minutes

CIP-003.R3 Challenges

- Data as a Critical Cyber Asset
- Decision Support systems
- Common control systems (aggregation)

CIP-002.R3 Challenges

- Rutable and Dial-up
 - Remove it, leave it, add new? **Be careful.**
- Rutable includes more than Ethernet...
 - Rutable: *both* network address and device address
 - Non-rutable: *only* device address
 - Fiber Channel Layer 2?
 - MPLS?



Western Electricity Coordinating Council

CIP-003 AC Evidence

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...*

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*

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)*

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

CIPUG CIP-003 Workshop

- 4/14/2009
- Denver, CO
- Grand Hyatt Denver
- <http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=304>
- *Still need asset owner volunteers!*



Western Electricity Coordinating Council

CIP-004 AC Evidence

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

Training vs. Awareness

- Note R1 (Awareness) is not part of the “First 13” in Table 1
- Awareness
 - Informal
 - No mandatory attendance records
- Training
 - Formal
 - Mandatory attendance records

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
 - Invoices

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
 - Invoices

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

CIPUG CIP-004 Workshop

- May, TBD
- Albuquerque, NM (unconfirmed)
- Stay tuned to CIPUG Upcoming Events page for details...
- <http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=304>
- *Still need asset owner volunteers!*



Western Electricity Coordinating Council

CIP-007 AC Evidence

CIP-007 Requirement 1

- *CIP-007.R1: Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.*
- Commonly evidenced by...
 - Test program/procedure documentation
 - Test results or records
 - Supporting documentation from other standards

CIP-007.R1.1 Evidence

- *The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.*
- Commonly evidenced by...
 - Formally documented test procedures
 - System configurations
 - Network diagrams

CIP-007.R1.2 Evidence

- *The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.*
- Commonly evidenced by...
 - Accurate system configurations
 - Accurate network diagrams

CIP-007.R1.3 Evidence

- *The Responsible Entity shall document test results.*
- Commonly evidenced by...
 - System configuration documentation
 - Test results/records
 - Supporting documentation from other standards

CIPUG CIP-007 Workshop

- 1/20/2009
- Mesa, AZ
- All presentation material including examples provided by the asset owner presenters can be found on CIPUG Previous Workshops page
- <http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=305>



Western Electricity Coordinating Council

CIP-008 AC Evidence

CIP-008 Requirement 1

- *CIP-008.R1: Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:*

CIP-008.R1.1 Evidence

- *Procedures to characterize and classify events as reportable Cyber Security Incidents.*
- Commonly evidenced by...
 - Formal incident response plan documentation
 - References to:
 - NERC Glossary
 - DOE-417
 - ES-ISAC

CIP-008.R1.2 Evidence

- *Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.*
- Commonly evidenced by formal incident response plan documentation

CIP-008.R1.3 Evidence

- *Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.*
- Commonly evidenced by...
 - Formal incident response plan documentation
 - Actual reports

CIP-008.R1.4 Evidence

- *Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.*
- Commonly evidenced by...
 - Formal incident response plan documentation
 - Policy language
 - Actual updates/revisions

CIP-008.R1.5 Evidence

- *Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.*
- Commonly evidenced by...
 - Formal incident response plan documentation
 - Policy/process language
 - Schedule and ownership for review of plan
 - Results of plan review

CIP-008.R1.6 Evidence

- *Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.*
- Commonly evidenced by...
 - Formal incident response plan documentation
 - Actual test scripts, results, schedule, etc
 - Policy/process language

CIPUG CIP-008/009 Workshop

- 3/18/2009
- Boise, ID
- The Grove Hotel
- <http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=304>
- *Still need asset owner volunteers!*



Western Electricity Coordinating Council

CIP-009 AC Evidence

CIP-009 Requirement 1

- *CIP-009.R1: Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:*

CIP-009.R1.1 Evidence

- *Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).*
- Commonly evidenced by...
 - Formal recovery plan documentation
 - Policy language

CIP-009.R1.2 Evidence

- *Define the roles and responsibilities of responders.*
- Commonly evidenced by...
 - Formal recovery plan documentation
 - Policy language

CIP-009 Requirement 2

- *CIP-009.R2: Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.*
- Commonly evidenced by...
 - Formal recovery plan documentation
 - Actual test scripts, results, schedule, etc
 - Policy/process language

CIPUG CIP-008/009 Workshop

- 3/18/2009
- Boise, ID
- The Grove Hotel
- <http://compliance.wecc.biz/Application/ContentPageView.aspx?ContentId=304>
- *Still need asset owner volunteers!*



Western Electricity Coordinating Council

WECC 2009 CIP Spot Check and Audit Plan

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 aspects is best

WECC RSAWs

- WECC CIP RSAWs (not NERC's version)
 - Will have have same content as NERC RSAWs, just reformatted for ease of use
 - Walk through the RSAW internally and map at least one evidence artifact to each requirement and sub-requirement
 - Two for good measure; corroborating evidence
 - Please no proprietary vendor questionnaires
 - Vendors should also use the RSAWs

Spot-Checks vs. Audits

- Very minor difference – the report
- Will be spot-checking all 13 requirements for all Table 1 entities in the AC phase between 7/1/09 and 7/1/10
- Will be a combination of off-site review and on-site review
- On-site review may take anywhere from 2 days to a full week

The On-Site Visit

- Small CIP-specific teams of 3-5 persons
 - May or may not be separate from Reliability Standard audits
- A WECC employee will lead spot check
- Will probably contain a NERC and/or FERC staffer
- Will need your CIP subject matter experts available for interviews, questions and supporting documentation

The On-Site Visit, Continued...

- Will follow all CMEP rules of engagement
- Will request non-sensitive information via Electronic Data Submittal in advance
- Will review sensitive information on-site, non-sensitive information off-site
- Where many systems or personnel are in scope, pseudo-random sampling techniques will be used

The On-Site Visit, Continued

- Electronic submittal of all evidence is required on Read-Only Memory (CD-ROM, DVD-ROM)
- All evidence on ROM must be hashed with SHA256, and hash [table] provided with evidence prior to submittal
- Spot check team will re-hash with SHA256 and verify; acceptance process

The On-Site Visit, Continued

- All evidence ROMs will be sealed in a signed envelope, and maintained at your facility of choice for duration of audit cycle
- The only paper document will be your list of Critical Cyber Assets
 - It will need to be physically signed in ink by your Senior Management Official, as designated in CIP-003.R2 and included in the sealed envelope

Post-Workshop Adjustment

- Two paper documents will be required
 - List of Critical Cyber Assets
 - Hash table(s) of all evidence submitted during spot check (or audit)
- Both will need to have a “wet” signature (ink) from the Senior Management Official or delegate

The On-Site Visit, Continued

- The only evidence that will be taken away is the SHA256 hash table(s) of evidence ROMs
- No sensitive information will leave with the auditors
- Any copied data will be “wiped” using 7-pass erasing technique (US DOD 5220.22-M 8-306)

Pre AC Spot-Check?

- Compliant (C) phase allows for spot-check, per CMEP...
- Would be for all of the First 13 in Table 1
- Would still be spot-checked during AC cycle/phase
- Any volunteers?

The Other Tables - 2, 3 and 4...

- Will not receive spot-checks or audits this cycle (7/1/09 – 7/1/10) – for now...
- Should proceed with any necessary self reports, mitigation plans, etc if not compliant
- All Tables are still bound to semi-annual self-certifications

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 required 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

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

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

Regional Consistency

- CIP Auditors from other Regions will participate in WECC spot-checks and audits
- CCWG – CIP Compliance Working Group
 - Compliance specific
- CIPMWG – CIP Managers Working Group
 - Not compliance specific
- www.RegionalEntities.org



Western Electricity Coordinating Council

CIP Horizon

Interpretations

- The NERC process is prohibitively difficult
- But still worth it...
- Helps everyone involved
- AOT [NERC] > CMPWG [Regions]
 - Audit Observation Team is now Compliance Monitoring Processes Working Group
- CMPWG releases approach guidance
 - www.regionalentities.org

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

*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
- Work is progressing quickly, expect something for review very soon
- Should be available for comment soon
- Will need to be complete before 7/1/09

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

CIP Compliance Tips

- Build a cross-functional team
 - Leverage Control Systems, Information and Physical Security, and DR/BCP experience
 - Listen to them and send their message upstream
- Be sensitive to Control Systems nuances
 - IT models may need to flex
 - Respect perspectives from both camps

CIP Compliance Tips, Continued...

- Change the way you do business
 - Don't just patch together existing documents from other standards/efforts
 - Demonstrate a true shift toward a more secure posture
- Design scalable solutions that can expand to meet new standards – they will change
 - Don't re-invent the wheel for every shift

CIP Compliance Tips, Continued...

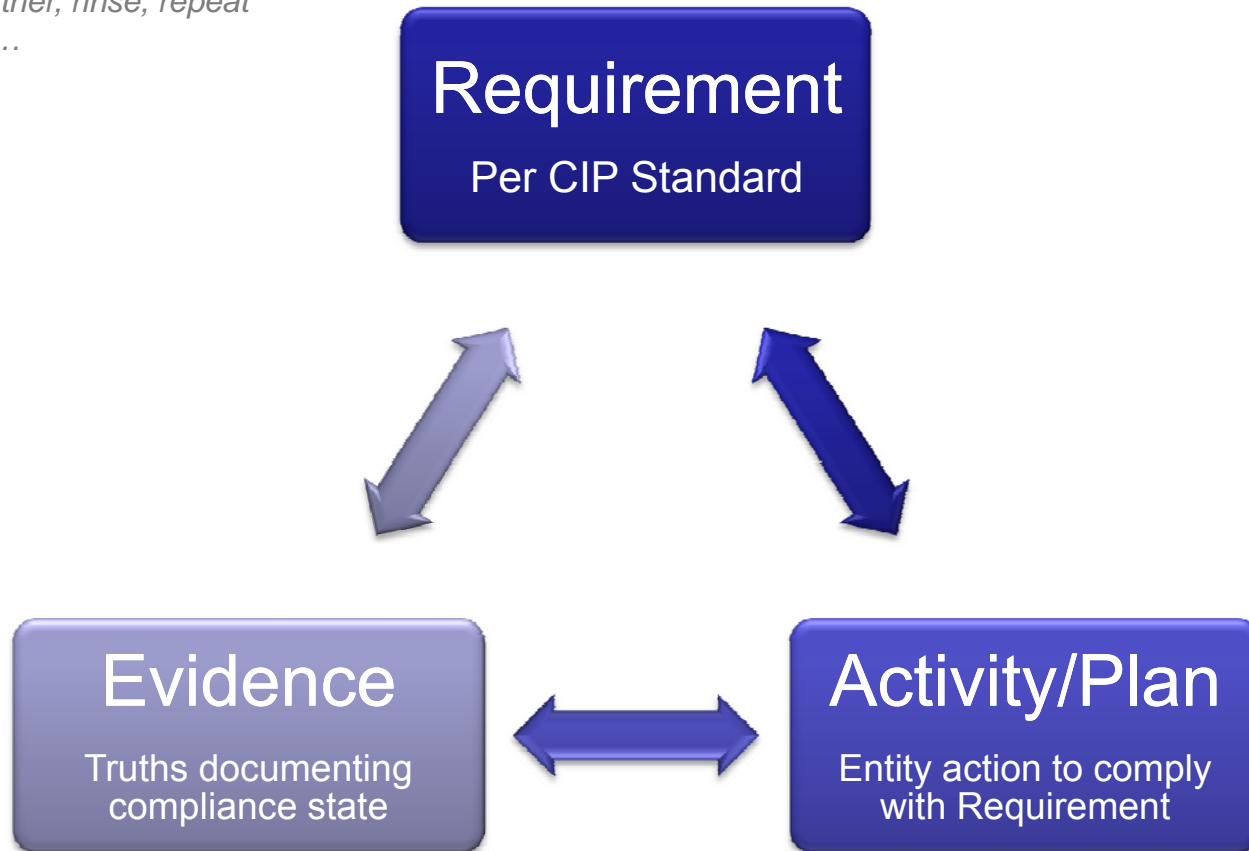
- Documentation is important!
 - Every word counts
 - Be aware of the differences between “shall” and “should”, “must” and “may”
 - Match language and documentation to standards wherever possible
 - Be mindful of signatures and dates

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
 - WICF – www.wicf.biz
 - E-SEC – www.energysec.org

Perpetual Compliance Cycle

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



CIP Crystal Ball

- Perfect Storm...
 - Technology shift
 - Media, media and more media
 - Unprecedented interest from the President, Congress and DHS
 - Other infrastructures (interdependencies)
- More restrictive regulations are likely
- Put on your seatbelt...

Current Events: Areva

- From US-CERT: <http://www.kb.cert.org/vuls/id/337569>

- I. Description

- AREVA e-terrahabitat is a core component of the Energy Management system that provides real-time data and process management services. e-terrahabitat contains vulnerabilities, including a buffer overflow. For more information on these issues AREVA customers should review the following issues in AREVA T&D Security Bulletin - ATD-08-002:
- PD28578 Buffer Overflow Vulnerability in e-terrahabitat MLF application
- PD32018 Denial of Service Vulnerability in e-terrahabitat WebFGServer application
- PD32020 Denial of Service Vulnerability in e-terrahabitat WebFGServer application
- PD32021 Denial of Service Vulnerability in e-terrahabitat NETIO application
- PD32022 Privilege Escalation in e-terrahabitat WebFGServer application
- Note that these issues affect versions 5.7 and earlier.

- II. Impact

- An unauthenticated attacker may be able to gain access with the privileges of the e-terrahabitat account or an administrator account and execute arbitrary commands, or cause a vulnerable system to crash.

- III. Solution

- Apply Patch: Users of e-terrahabitat version 5.5, 5.6, and 5.7 should apply the e-terrahabitat_560_P20081030_SEC patch immediately.
- Upgrade: Users of affected software with versions 5.4 and earlier are encouraged to upgrade to 5.6 or above.

Current Events: Rockwell

- Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge - <http://www.kb.cert.org/vuls/id/882619>
 - Cross-site scripting vulnerability
- Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge URL - <http://www.kb.cert.org/vuls/id/619499>
 - Redirection vulnerability
- GoAhead Webserver information disclosure vulnerability - <http://www.kb.cert.org/vuls/id/124059>

Vulnerability Treadmill...

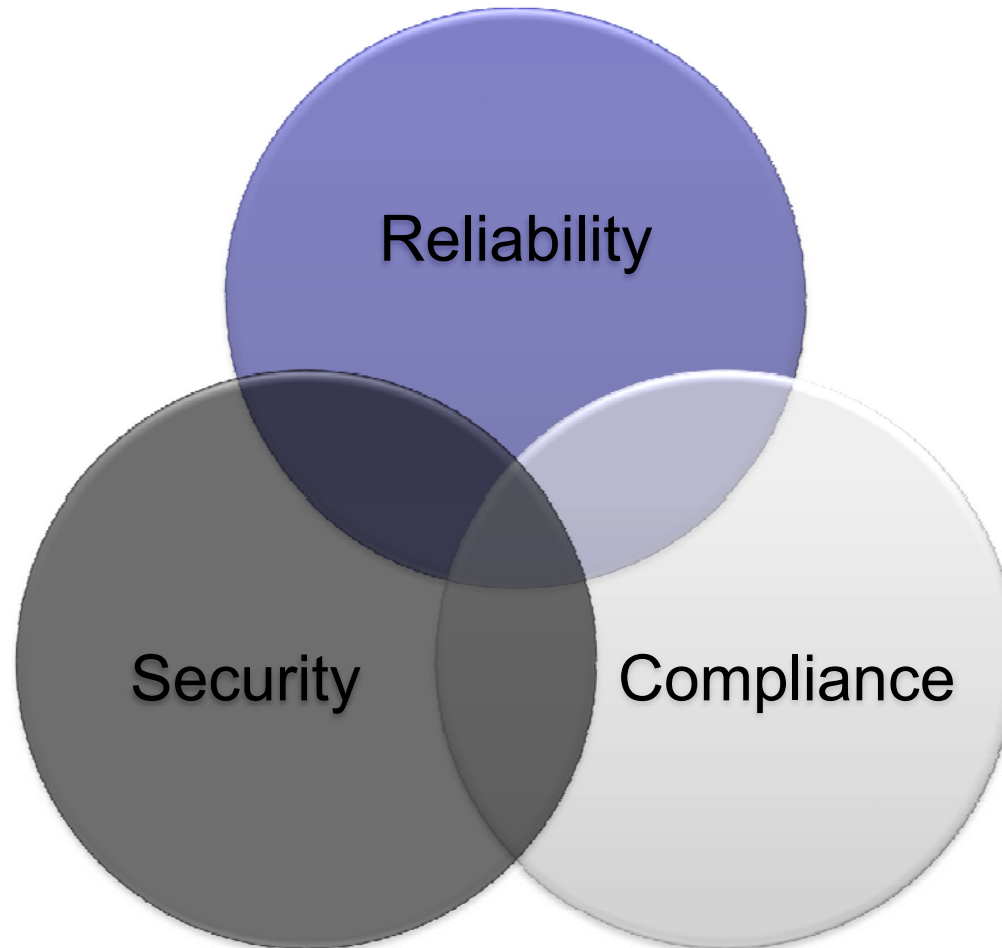
- Rumors of many more (from SANS event last week)...
 - GE Fanuc iFIX HMI
 - Some details were published, but immediately redacted after public availability
- SCADA vulnerability research is now mainstream; expect more
- Willie Sutton: “*because that’s where the money is*”

Compliance vs. Security

- The 7 Dirty Little Secrets of the Security Industry* ...
 - “#5. Compliance threatens security. Compliance in and of itself is not a bad thing. But, compliance in and of itself does not equal security. At the very least it's a resource and budget conflict, and it splits our focus. Compliance is supposed to raise the minimum standard of security, but it just gets us to do what we are required to do and nothing else.
 - “What's more, that which is easy to measure is not necessarily that which is most valuable. So if there were 15 software vulnerabilities last month, we can measure that 12 of them have been patched. It is much harder to measure how effective end user training was to make administrators immune to social engineering attacks. The lesson is you need to be compliant, but your entire risk strategy cannot be based on it.”

* http://www.infoworld.com/article/09/01/28/The_7_dirty_secrets_of_the_security_industry_1.html

The Big Picture



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.

Volunteer Reminder

- CIPUG Workshops
 - 008/009 - Boise
 - 003 - Denver
 - 004 – TBD (Albuquerque?)
- Electronic Data Submittal
- Spot check

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
503.260.6472 (m)
360.567.4056 (d)

Bill Fletcher
Compliance Engineer, Cyber Security
Western Electricity Coordinating Council
7600 NE 41st Street, Suite 160
Vancouver, WA 98662
wfletcher@wecc.biz
541.912.3226 (m)
360.567.4061 (d)

Taud Olsen
Director, Stakeholder Relations and
Compliance Outreach
615 Arapeen Drive, Suite 210
Salt Lake City, UT 84108-1262
tolsen@wecc.biz
801.883.6894 (m)
801.819.7603 (d)

Resources And References

- SCADA Procurement Language
 - <http://www.msisac.org/scada/>
- OCTAVE Allegro
 - <http://www.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf>
- NIST / Process Control Security Requirements Forum Resource
 - <http://www.isd.mel.nist.gov/projects/processcontrol/members/resources.html>
- National Checklist Repository
 - <http://checklists.nist.gov/>
- NIST Special Publications 800 Series
 - <http://csrc.nist.gov/publications/PubsSPs.html>
- NERC Glossary of terms used in Reliability Standards
 - http://www.nerc.com/files/Glossary_12Feb08.pdf
- NERC CSO706SDT / CIPv2, v3...
 - http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Check often, standard disclaimers apply...