



*Western Electricity Coordinating Council*

# CIP-002 Workshop

---

NWPPA, PNGC and WECC

Sheraton Portland Airport, Portland, OR

April 30th, 2008 - **Updated 5/19/2008**

Patrick Miller CISA CISSP-ISSAP

WECC Sr. Compliance Engineer, Cyber Security

# Workshop Overview

---

- Introduction
- Surveys
- CIPS Ramp Up
- CIP-002.R1-R2 Walkthrough
- CIP-002.R3 Guidance
- WECC Updates
- NERC Updates
- CIP Crystal Ball

# Scope and Disclaimer

---

- This workshop is intended to provide assistance for small-to-mid sized electric utilities in their understanding of CIP-002
- None of the information shared and discussed within this workshop is intended to act as a guarantee of compliance, in whole or in part, for any of the CIP standards
- No information from this effort may be used for competitive purposes

# Introduction

---

- Patrick Miller

- CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM
- 20+ years in IT
- 8+ years in Electric Sector
- Sr. Compliance Engineer, Cyber Security
- I will be your WECC CIP Auditor

# Surveys

---

- Question One: 4
- Question Two: range
- Question Three: range
- Question Four: 3
- Question Five: 1
- Question Six: 2
- Question Seven: 3
- Question Eight: 5
- Question Nine: 3



*Western Electricity Coordinating Council*

# CIPS Ramp Up

---

# CIPS In A Nutshell...

---

- Critical Infrastructure Protection Standards (CIPS) are intended to protect the following:
  - Bulk Power System (Bulk Electric System)
  - Critical Assets
    - Control Centers, Transmission Subs, Generation Plants
  - Critical Cyber Assets
    - EMS, DCS, RTUs, IEDs, PLCs, Relays
    - Decision Support Systems
  - Critical Infrastructure Information
- Provide greater reliability through greater security and accountability
  - Must be able to confirm who did what, and when...

# CIP Past to Present

---

- FERC SMD Appendix G
  - NERC UAS-1200
  - NERC 1300
  - NERC CIP 002-009
  - NERC CIP-001
  - FERC Order 693
  - FERC Staff Assessment
  - FERC CIPS NOPR
  - FERC Order 706
- Influential Factors
    - Interdependency studies
    - NE Blackout 2003
    - “Aurora” DPCD issue
    - SANS CIA briefing
    - News media in general



*Western Electricity Coordinating Council*

# CIP-002.R1-R2 Walkthrough w/ RAWG Draft v2

---

# CIP-002 – High Level Overview

---

- R1: Adopt a methodology
  - Pick one, create one, borrow one - and document it
  - Quality counts
- R2: Critical Asset List
  - Focus on all facilities that are part of the BPS
  - Impact Analysis vs. Risk-Based Methodology
  - Risk to the BPS is the real question
  - Redundancy doesn't count
- R3: Critical Cyber Asset List
  - Don't forget Decision Support Systems
  - EMS, DCS, RTUs, IEDs, PLCs, Relays
  - Redundancy doesn't count
- R4: Annual Approval

# NERC RAWG CIP-002 Guideline

---

- Directed by FERC in Order 706
- NERC Risk Assessment Working Group
- Second guideline effort
- Vastly more effective than first round
- Highly actionable information
- Following ANSI accredited process (slow)
- Information provided today is from the DRAFT second version
- Please participate via comments

# NERC RAWG CIP-002 Guideline

---

- The following details are considered to be generally accepted good practice guidelines for the determination of Critical Assets
- This is not intended to be a the authoritative source for Critical Asset determination
- The RAWG guidelines are not yet final, as such expect more refinement before guidance is “final”

# RAWG Guideline Preamble/Scope

---

- “Guidelines provide suggested guidance on a particular topic for use by bulk electric system entities according to each entity’s facts and circumstances and not to provide binding norms, establish mandatory reliability standards, or be used to monitor or enforce compliance.”
- “The criteria in this guideline are not requirements, nor should they be construed as such. This guideline does not supersede reporting requirements for power system operation or as required by law.

# CIP-002 Guidelines

---

- Two volume set
  - First volume is a methodology to identify Critical Assets essential to the reliable operation of the Bulk Power System
  - The second volume provides a methodology to identify which, if any, of the Cyber Assets associated with each Critical Asset are essential to their operation, and therefore qualify as Critical Cyber Assets

# BES vs. BPS

---

- NERC = BES; FERC = BPS
- BPS going forward
- Specific exclusion per FERC for Distribution
- Essentially interchangeable

Risk...



# 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

# Risk vs. Impact Analysis

---

- Assume the threat exists
- Assume vulnerability exists
- Set probability to 100% or 1
- New result: Risk = Impact (ignore probability)
- Risk analysis translates into an impact analysis instead
- “Does an asset if destroyed, degraded, compromised or otherwise rendered unavailable, impact the reliability of the Bulk Power System?”

# Guideline Approach

---

- A. Determination of asset types that need to be evaluated
- B. Defining Assets
- C. Application of evaluation criteria
- D. Listing Critical Functions
- E. Documentation of Assessment

# (A) Determining Asset Types

---

- A. Determination of asset types that need to be evaluated
- B. Defining Assets
- C. Application of evaluation criteria
- D. Listing Critical Functions
- E. Documentation of Assessment

# (A) Determining Asset Types

---

- Start with list of all BPS assets owned
  - If shared ownership, one owner must be designated as the responsible party
- Compile list of which assets need to be evaluated to determine if they are Critical
- Identify Critical Assets at the facility level
  - Exception is special systems not subordinate to a facility but still impacting BPS

# (A) Determining Asset Types

---

- Transmission substations
  - Facilities performing electrical Element switching, transforming voltage, regulating power or metering BPS Elements

# (A) Determining Asset Types

---

- Generation resources

- Individual generating unit  $> 20$  MVA (gross nameplate rating) and is directly connected to the BPS
- Generating plant/facility  $> 75$  MVA (gross aggregate nameplate rating) or when the entity has responsibility for any facility consisting of one or more units that are connected to the BPS at a common bus with total generation above 75 MVA
- Any generator, regardless of size that is a blackstart unit material to and designated as part of a transmission operator entity's restoration plan
- Any generator regardless of size that is material to the reliability of the BPS

# (A) Determining Asset Types

---

## ● Control Centers

- Control centers housing primary or backup control systems that are used to monitor and/or operate BPS equipment should be evaluated
- Facilities that perform one or more of the functions listed below for other multiple, geographically separated BPS assets:
  - Supervisory control of BPS assets, including generation plants, transmission facilities, substations, AGC and automatic load shedding systems
  - Data acquisition, aggregation, processing transfer and display
  - BPS system status monitoring and processing for reliability and asset management purposes
  - Alarm monitoring and processing

# (A) Determining Asset Types

---

- Systems

- If/where not already included, systems separate from the primary function of a facility but have the ability to impact the BPS
  - Network-wide situational awareness
  - supervising and control capability
  - BPS restoration or emergency stability capability should be considered critical assets regardless of the number of Critical Assets with which these systems interact

# (B) Defining Assets

---

- A. Determination of asset types that need to be evaluated
- **B. Defining Assets**
- C. Application of evaluation criteria
- D. Listing Critical Functions
- E. Documentation of Assessment

## (B) Defining Assets

---

- Critical Assets should be identified at the BPS facility level
- Special systems not subordinate to a facility but connected to or existing on a facility that can impact the BPS should be identified
- If degradation of a facility or separate system affects the reliability of the BPS, then that facility or system should be considered a Critical Asset

## (B) Defining Assets

---

- Critical Assets can be defined at the system level, but..
- Systems or equipment that are elements of a facility that is identified as a Critical Asset and support its functions are not intended to be identified separately from the facility itself
- Some systems may end up being Critical Assets and Critical Cyber Assets

# (B) Defining Assets

---

- Common Mode Impacts
  - Considered to happen at the facility, unit and system level
  - Facility e.g.: automatic load shedding systems spanning facilities
  - Unit e.g.: support systems spanning units such as control systems or shared networks
  - System e.g.: support systems spanning primary systems within a facility

## (B) Defining Assets

---

- Control Centers should be evaluated as potential Critical Assets, except...
- Control Centers that are collocated with one or more other BPS assets should still be evaluated separately from the other assets, except...
- Single-asset Control Centers or Control Centers that perform supervisory control and/or monitoring functions for a single BPS asset

# (C) Evaluation Criteria

---

- A. Determination of asset types that need to be evaluated
- B. Defining Assets
- **C. Application of evaluation criteria**
- D. Listing Critical Functions
- E. Documentation of Assessment

# (C) Evaluation Criteria

---

- Criteria along with reasonable bases for the determination of Critical Asset are provided for:
  - Substations
  - Generators
  - Control Centers
  - Special Systems
- Note that redundancy of a Critical Asset doesn't count and should not be used as evaluation criteria

# (C) Evaluation Criteria

---

- Substations

- Criteria: Essential to restoration

- Example Bases:

- The substation is identified in a Cranking Path document in the regional system restoration plan (EOP-005-01)

# (C) Evaluation Criteria

---

- Substations

- Criteria: Essential to critical generation

- Example Bases:

- Loss of substation, as determined by an engineering evaluation may result in:
  - Loss of generation identified as a Critical Asset
  - ...or, event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417 (generation loss of 2000 MW or more)
  - ...or, System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) violation (FAC-011-01)
- Nukes refer to NUC-001 and (NPIRs)

# (C) Evaluation Criteria

---

- Substations

- Criteria: Essential for voltage support

- Example Bases:

- Loss of substation, as determined by an engineering evaluation may result in:

- An event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417

- Sustained voltage excursions equal to or greater than 10%
- Frequency or voltage going below the UF or UV load shed points
- System wide voltage reductions of 3% or more

- ...or, System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) Violation (FAC-011-01)

# (C) Evaluation Criteria

---

- Substations

- Criteria: Essential for frequency support

- Example Bases:

- Loss of substation, as determined by an engineering evaluation may result in:

- An event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417

- Frequency or voltage going below the UF or UV load shed points

# (C) Evaluation Criteria

---

- Substations

- Criteria: Essential for system stability

- Example Bases:

- Loss of substation, as determined by an engineering evaluation may result in:

- o An event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417

- Complete operational failure/shutdown of the transmission system
- Diminished system restoration capability
- Transmission line thermal limits exceeded beyond 135% of normal
- Impact to reliability of neighboring system

- o ...or, System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) Violation



# (C) Evaluation Criteria

---

- Generators

- Criteria: Essential to loss generation

- Example Bases:

- Loss of either single or combined units (subject to common mode failure) exceeding the regional reliability threshold for 80% of the single largest contingency w/ reference to BAL-002
- ...or, loss of substation, as determined by an engineering evaluation may result in an event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417
- ...or, loss of generation by a GO, BA, or LSE of 2,000MW or more

# (C) Evaluation Criteria

---

- Generators

- Criteria: Essential to voltage support

- Example Bases:

- Loss of either single or combined units (subject to common mode failure) as determined by an engineering evaluation may result in an event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417
  - Sustained voltage excursions equal to or greater than +/- 10%
  - Frequency or voltage going below the UF or UV load shed points
  - System wide voltage reductions of 3% or more
- ...or, loss of single or combined units (subject to common mode failure) at a generation plant, as determined by an engineering evaluation, may result in a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) violation (FAC-001-01)

# (C) Evaluation Criteria

---

- Generators

- Criteria: Essential to frequency response

- Example Bases:

- Loss of either single or combined units (subject to common mode failure) as determined by an engineering evaluation may result in an event within the disturbance reporting criteria identified in EOP-004-01 or DOE EIA 417

- o Frequency or voltage going below the UF or UV load shed points

# (C) Evaluation Criteria

---

- Generators

- Criteria: Essential to constraint mitigation

- Example Bases:

- Unit or plant generation that has been determined essential to the BPS reliability through an engineering study and deemed “must run for reliability” is to be considered Critical
  - To the extent that the “must run for reliability” determination was a system study and not a product caused by market created flows
- ...or, loss of the generation as determined by an engineering evaluation, may result in a System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) violation (FAC-001-01)

# (C) Evaluation Criteria

---

- Generators

- Criteria: Essential to “Black Start”

- Example Bases:

- Generating units considered Black Start units expected to perform functions as specified in overall coordinated Regional Systems restoration plans are to be considered Critical
- EOP-007 with applicability to EOP-005 and EOP-008

# (C) Evaluation Criteria

---

- Control Centers

- Criteria: Essential by virtue of their functions to the BPS
- Example Bases:
  - Primary and backup Control Centers owned, operated or employed by a BA, IA or RC

# (C) Evaluation Criteria

---

- Control Centers

- Criteria: Essential for providing information used by the Responsible Entities to make operational decisions regarding BPS reliability
- Example Bases:
  - Loss of collection, aggregation, processing, display, or alarm of data or information from a primary or backup Control Center to a Responsible Entity determined by an engineering study to negatively affect the reliability of the BPS

# (C) Evaluation Criteria

---

- Control Centers

- Criteria: Essential for inter-utility data exchange critical to reliable BPS operation
- Example Bases:
  - Loss of inter-utility data exchange from the primary or backup Control Center determined by engineering evaluation to negatively impact the reliability of the BPS.

# (C) Evaluation Criteria

---

- Control Centers

- Criteria: Essential for control or data acquisition to BPS asset determined to be a Critical Asset
- Example Bases:
  - Loss of supervisory control or data acquisition function for a BPS asset determined to be a Critical Asset.

# (C) Evaluation Criteria

---

- Control Centers

- Criteria: Essential for control or data acquisition for a set of BPS assets determined collectively to be critical to reliable BPS operation
- Example Bases:
  - Loss of supervisory control or data acquisition function for a set of BPS assets determined collectively to be critical to reliable BPS operation.

# (C) Evaluation Criteria

---

- Special Systems

- Criteria: Essential to the Remedial Action Scheme (RAS) or Special Protection System (SPS)
- Example Bases:
  - The facility has specific equipment use or designations supporting the BPS
  - The substation is part of a RAS/SPS system as identified in internal system operating bulletins, regional system protection documentation or other authoritative sources

# (C) Evaluation Criteria

---

- Special Systems

- Criteria: Essential by virtue of their functions to the BPS
- Example Bases:
  - The facility has specific equipment use or designations supporting the BPS
  - Engineering evaluation determine asset to be critical to reliable operation of the BPS

# (D) Listing Critical Functions

---

- A. Determination of asset types that need to be evaluated
- B. Defining Assets
- C. Application of evaluation criteria
- **D. Listing Critical Functions**
- E. Documentation of Assessment

# (D) Listing Critical Functions

---

- For facilities and systems determined to be Critical Assets, critical functions should be identified
  - For facilities that perform more than one critical function, all critical functions should be identified
  - Identification of critical functions for a facility can be done by listing which Evaluation Criteria were met
  - Identification is important for the further assessment of Critical Cyber Assets

# (D) Listing Critical Functions

---

- Asset functions should be compared to the following list of functions generally considered to be important to the reliability of the BPS:
  - Generator control or AGC
  - Breaker or transformer control
  - Voltage
  - Load Shedding
  - Real time Monitoring
  - System Monitoring and Alarming
  - Inter-utility data exchange
  - System Protection

# (E) Documentation of Assessment

---

- A. Determination of asset types that need to be evaluated
- B. Defining Assets
- C. Application of evaluation criteria
- D. Listing Critical Functions
- E. Documentation of Assessment

# (E) Documentation of Assessment

---

- The evaluation should be performed in consultation with system operators and planners using system studies, analysis, simulations and/or historical experience
- The evaluation and bases for the judgements made about whether assets meet particular criteria should be documented

# (E) Documentation of Assessment

---

- Documentation of the evaluation should include:
  - Identification of the assets considered
  - Identification of the assets considered to be Critical Assets
  - Justification or bases for why assets were or were not considered to be Critical Assets
  - Listing of all critical functions that each Critical Asset performs

# (E) Documentation of Assessment

---

- Reasonable bases supporting an evaluation include:
  - Engineering evaluations
  - Authoritative studies
  - Specific equipment use or designations that support the BPS

# (E) Documentation of Assessment

---

- Engineering Evaluations
  - To determine the extent to which an asset supports reliable operation of the BPS, system simulations and associated assessments should be performed in accordance with the requirements identified in TPL-004
  - Engineering assessments and simulations should evaluate impact under extreme conditions such as those identified as Category D disturbance criteria

# (E) Documentation of Assessment

---

- Authoritative Studies and Sources
  - Existing authoritative studies and sources may be utilized to determine whether or not a facility is essential to performing function(s), for example:
    - Regional transmission planning studies
    - System operating bulletins
    - NERC documentation

# (E) Documentation of Assessment

---

- Specific Equipment Use or Designations Supporting the BPS
  - Signify critical support to the BPS, for example:
    - Generation output greater than largest single contingency for the area
    - Presence of reliability must run capacitors
    - Static Var Compensation mechanisms

# Other Options

---

- Prior RAWG recommendations

- <http://www.esisac.com/library-assessments.htm>
- EEI Security Committee Approach
- DHS Risk Analysis and Management Approach
- AS/NZS 4630:2004
- DOE VRAM
- RAM D/T
- PNNL Risk Communication Assessment and Prioritization Program
- AEP Attack Tree Methodology
- EPRI Security Vulnerability Self-Assessment

- OCTAVE Allegro

- Suggestions?



Western Electricity Coordinating Council

# CIP-002.R3: Critical Cyber Asset Identification

---

# CIP-002.R3 Guidance

---

- NERC RAWG guidance document for identification of Critical Cyber Assets is in the earliest stages of development and as such, there is no functional working draft to use at this time
- The following guidance is generally accepted practice
- This is not intended to be a the authoritative source for Critical Cyber Asset determination

# What is a Critical Cyber Asset?

---

- Systems and facilities at master and remote sites that provide:
  - Monitoring and control
  - Automatic Generation Control
  - Real-time power system modeling
  - Real-time inter-utility data exchange
  - Protection (DPCD; Relays)
  - Decision support
  - Data

# What is a Critical Cyber Asset?

---

- Must use a routable protocol to communicate outside the Electronic Security Perimeter
  - OSI layer 3 or higher (Frame Relay is Layer 2 and is out of scope)
  - Profibus, DNP, Modbus, Fieldbus, etc to do not explicitly use Layer 3 and are out of scope unless “wrapped/tunneled” in IP (“...over IP”)
- Uses a routable protocol within a Control Center

# What is a Critical Cyber Asset?

---

- Dial-up accessible
  - Any temporary (non-permanent), interruptible, or not continuously connected communication access to a Critical Cyber Asset from any remote site
  - VPN and Wireless are considered dial-up
  - Dedicated communication circuits are out of scope

# What is not a Critical Cyber Asset?

---

- Communications systems
  - Leased lines
  - Outside of the Electronic Security Perimeter
- Environmental systems (HVAC, UPS)
  - Except those which are network connected within the Electronic Security Perimeter
- Alarm systems
  - Environmental, support or communications
  - Except where they provide critical operating functions or tasks



*Western Electricity Coordinating Council*

# CIP-002.R4: Annual Approval

---

# Annual Approval

---

- Annual approval of the results of the annual application of the risk based methodology to determine Critical Assets and Critical Cyber Assets must be performed and documented
- Senior Manager or delegate must provide approval statement
- Approval statement must be signed and dated



Western Electricity Coordinating Council

# WECC Updates

---

# WECC Updates Overview

---

- Extensive outreach effort
- Compliance Portal
- Compliance Website
- Cyber security webpage

# WECC CIP Outreach

---

- Open Mic calls dedicated to CIP issues
- Email CIP questions to [pmiller@wecc.biz](mailto:pmiller@wecc.biz)
- CUG Meetings
- CIPUG Meetings
- Workshops on specific standards
- Dedicated Cyber Security page on website
- Living Cyber Security FAQ on website

# Compliance Portal

---

- To be used by all Registered Entities
- Each entity will have their own section
- Entities will manage compliance documentation and dates
- Secure mechanism to submit compliance evidence and complete forms
- “Train the trainer” will happen soon
- Should be released within the next two months or so

# Compliance Website

---

- Public information; different than portal
- All items (and more) from the existing Compliance pages on WECC website
  - Documentation
  - Forms
  - Calendar
  - Etc...
- Dedicated cyber security page

# Cyber Security Webpage

---

- WECC Cyber Security
  - Mission statement(s) - WECC's Cyber Security commitment
  - Cyber Security related items on the WECC Calendar (compliance dates, open mic calls, training, outreach, etc)
  - Submit a Cyber Security question
  - FAQ for common security questions to WECC
  - WECC Cyber Security blog/news-headlines
  - All WECC Security guidelines and policies
- Cyber Security Regulations and Standards
  - NERC CIP Standards
  - FERC Order 706

# Cyber Security Webpage

---

- Forums, Working Groups and Committees
  - WECC: CIPUG, CUG, PSWG, DEWG, EMSWG
  - NERC: CSSWG, CIPC
  - DHS: PCSF, US-CERT ES-Portal
  - Industry: E-Sec NW, EEI Security Committee, APPA, NWPPA
- Useful Cyber Security Resources
  - NERC ES-ISAC (includes all guidelines as well as RAMs, etc)
  - NIST SP800 series
  - ISA-SP99
  - ISO27001
  - US-CERT
  - Cyber Security Procurement Language for Control Systems
  - National Labs: PNL, INL, SNL
  - Find your local FBI contact
  - Find your local DHS PSA



# NERC Updates

---

# NERC Updates

---

- Implementation Plan
- Penalties and Sanctions
- CIP RSAWs
- Auditor Training

# Implementation Plan

---

- NERC has released guidance on the usage and interpretation of the Implementation Plan at:

[ftp://www.nerc.com/pub/sys/all\\_updl/standards/Guidance\\_on\\_CIP\\_Standards.pdf](ftp://www.nerc.com/pub/sys/all_updl/standards/Guidance_on_CIP_Standards.pdf)

# Implementation Plan - Table 1

**Table 1**  
**Compliance Schedule for Standards CIP-002-1 through CIP-009-1**  
**Balancing Authorities and Transmission Operators Required to Self-certify to UA**  
**Standard 1200, and Reliability Coordinators**

Requirement	End of 2 <sup>nd</sup> Qtr 2007		End of 2 <sup>nd</sup> Qtr 2008		End of 2 <sup>nd</sup> Qtr 2009		End of 2 <sup>nd</sup> Qtr 2010	
	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
<b>Standard CIP-002-1 — Critical Cyber Assets</b>								
R1	SC	BW	C	SC	AC	C	AC	AC
R2	SC	BW	C	SC	AC	C	AC	AC
R3	SC	BW	C	SC	AC	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC

# Table 1 Applicability

---

- Balancing Authorities and Transmission Operators required to self-certify to UAS1200 (previously monitored for compliance as Control Areas\*) and Reliability Coordinators

\* [http://www.nerc.com/~filez/standards/Cyber\\_Sec\\_Renewal.html](http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html)

# Table 1 - the First 13

---

- 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 (Electronic Security Perimeter) and CIP-006 (Physical Security) have no “Compliant” requirements for the 6/30/08 deadline

Also note that compliance to CIP-001 is already required

# Implementation Plan - Table 4

**Table 4**  
**Compliance Schedule for Standards CIP-002-1 through CIP-009-1**  
**For Entities Registering in 2007 and Thereafter.**

	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
<b>Standard CIP-002-1 — Critical Cyber Assets</b>				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC

# CIP Compliance Phases

---

- [BW, SC] Before Compliant stage, semi-annual self-certifications will be conducted
- [C] Compliant Stage (on or after 7/1/08)
  - All CIP Standards will be included in the Actively Monitored list of standards
  - Only self-certification, self-reports, investigations
  - No audits or spot-checks until AC stage
- [AC] Auditably Compliant Stage (on/after 7/1/09)
  - Subject to audits and spot checks

# Pre-Compliant Stage

---

- **Begin Work (BW)** - Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements
- **Substantially Compliant (SC)** - Entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant

# Semi-Annual Self-Certifications

---

- Only for BW and SC compliance phases
- Semi-Annual self-certifications to start July 1<sup>st</sup> and January 1<sup>st</sup>; starting July 1<sup>st</sup>, 2008
- WECC will be following up on inconsistent/insufficient responses and non-response to prior self-certifications

# Semi-Annual Self-Certifications

---

- WECC will send the semi-annual self-certification forms to the Registered Entities around mid-June, to be filed with WECC by mid-July
- A Registered Entity indicating it has not reached the milestone for a requirement will be required to submit a mitigation plan

# Compliant Phase

---

- Compliant (C) - Entity meets the full intent of the requirements and is beginning to maintain required “data,” “documents,” “documentation,” “logs,” and “records”

# Compliant Phase - Monitoring

---

- Requirements are subject to partial CMEP:
  - Spot Checks for cause
  - Self-Report
  - Self-Certification
  - Investigations
  - Periodic Reports
  - Penalties and Sanctions
- No audits (on-site or off-site) until 7/1/09

# Auditably Compliant Phase

---

- One full year of compliance evidence
- Requirements are subject to full CMEP:
  - Audits (on-site and off-site)
  - Routine Spot Checks
  - Self-Report
  - Self-Certification
  - Investigations
  - Periodic Reports
  - Penalties and Sanctions

# Penalties and Sanctions Changes

---

- Penalties and Sanctions can be levied upon the Compliant (C) phase
- Entities that feel they will not make the Compliant date for the first 13 requirements in Table one can submit a self-report with a mitigation plan and receive “regional discretion” for penalties and sanctions

# CIP RSAW

---

- What are Reliability Standards Audit Worksheets?
- First cut will be only for the first 13 requirements (7/1/08)
- Being developed by NERC and SMEs from the RROs
- Should be “draft complete” after 5/1/08
- Will be “final” by (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 expected
  - Use the RSAWs and Yellow Book
  - Get trained by ISACA and IIA



*Western Electricity Coordinating Council*

# CIP Crystal Ball

---

# CIP Future

---

- FERC

- FERC (and HSC) want a more prescriptive and restrictive standard going forward
- NIST 800-53/800-82 may be the goal

- NERC

- New CIPS drafting team is formed to revise existing CIP Standards per FERC directives
- CIP-010, 011 and 012...

- A security-related event may accelerate changes or new standard development

# CIP Compliance Tips

---

- Get the CIP-002 effort done first, then run other initiatives in tandem/parallel where possible
- Leverage Control Systems, Information and Physical Security, and DR/BCP experience
- Design scalable solutions that can expand to meet new standards – they will change
- Defense in depth is best; can demonstrate intent
- Don't forget about sensitive information/data
- Talk to your peers and find out what works
- Use the RSAW and Implementation Plan

# Upcoming Events

---

- WECC CUG
  - June 9-11, Marriott Downtown Waterfront
  - Portland, OR
- WECC CIPUG
  - June 12-13, Doubletree Lloyd Center
  - Portland, OR
- E-Sec NW CIPS Summit
  - July 23-24, Doubletree Lloyd Center
  - Portland, OR

# Questions?



Patrick Miller CISA, CISSP-ISSAP  
Sr. Compliance Engineer, Cyber Security  
Western Electricity Coordinating Council  
7600 NE 41<sup>st</sup> Street, Suite 160  
Vancouver, WA 98662  
360.567.4056 (d) / 503.260.6472 (m)