

RELIABILITY COMPLIANCE

NWHA Annual Conference, March 19, 2009

Crystal Musselman
Director, Compliance Outsourcing Services
Intellibind, LLC.

Outline

- How did we get here?
 - Crystal Musselman
- Cyber Security Standards
 - Adam Menendez and Matt Jastram
- Where are we headed?
 - Alan Cooke

Opinions

- The opinions and comments are those of Crystal Musselman, Adam Menendez, Matt Jastram, and Alan Cooke, not those of our respective companies

NERC Reliability Standards History

- The electricity industry has had planning and operating criteria for decades, but compliance was always voluntary
- In August 2003, a blackout that affected 50 million people in the northeastern and mid-western U.S. and Canada, prompted U.S. legislators to make standards mandatory via the Energy Policy Act of 2005
- This major shift in industry regulation resulted in Order 693 issued in March 2007

NERC Reliability Standards History

- On March 15, 2007 FERC approved 83 NERC Reliability Standards and 6 regional differences, the first set of legally enforceable standards for the U.S. bulk power system
- June 18, 2007 mandatory Reliability Standards in the United States
 - Authority to levy financial penalties – up to \$1,000,000 per violation, per day

Definition

- A reliability standard defines obligations or requirements of utilities and other entities that operate, plan and use the bulk power system in North America
- The Bulk Electric System -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.

Who Does What?

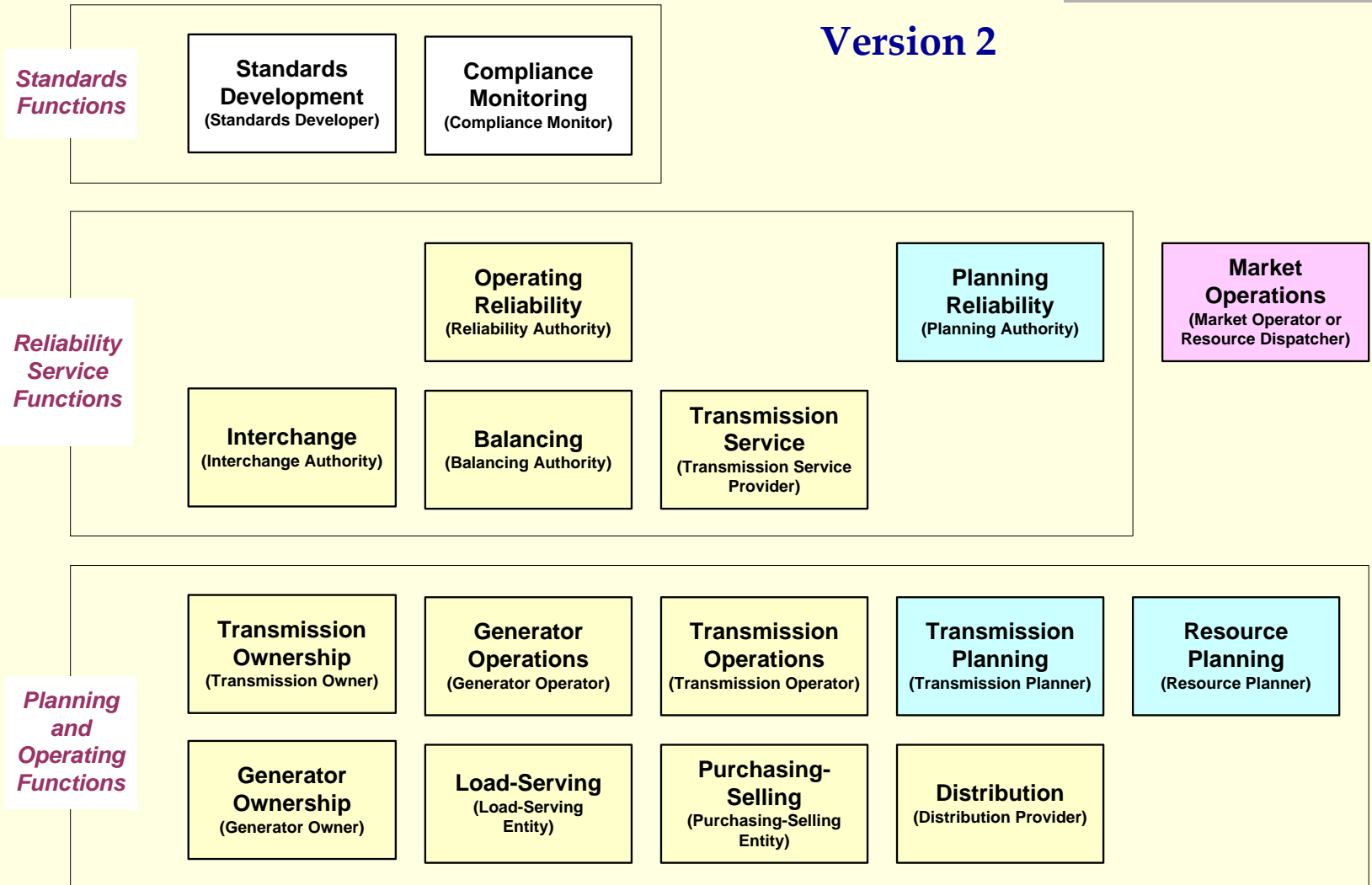
- FERC
 - 2005 EPA gave FERC authority over Reliability Compliance
- NERC (ERO)
 - Write the Reliability Standards
- WECC (RRO) – one of 8 regions
 - Monitor and Audit compliance with the Reliability Standards
- Registered Entity – Users, Owners, Operators of BES

Entity Registration

- Registered Entity
- Joint Registration Organization
 - Joint Agency
 - Multiple Entities
 - Split functions
 - **Requirements**
 - **Documentation**

Functional Model

Version 2



Generator Owner

- The Generator Owner owns its generation facilities and provides for the maintenance of those facilities.

Generator Operator

- The Generator Owner may operate its generating facilities or designate a separate organization to perform the Generator Operations Function.
- The Generator Operator operates, or directs the operation of generation facilities.

Registered Entity GO and GOP

- Internal Reliability Compliance Program
 - Plan
 - Culture of Compliance
 - Dedicate Resources

- 6 year audit cycle - Table-top
 - Unless also registered as BA/TOP/TOP
 - June 30 Self-Certification
 - July 15 Spot Check
 - CIP Semi-annual

Cyber Security Standards (CIP)

- To ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric System.

Cyber Security Standards (CIP)

- Implementation Plan
 - Table 3 & 4 (registration date)

- CIP-003 R2
 - Compliant by December 31, 2008
 - Assign Senior Manager

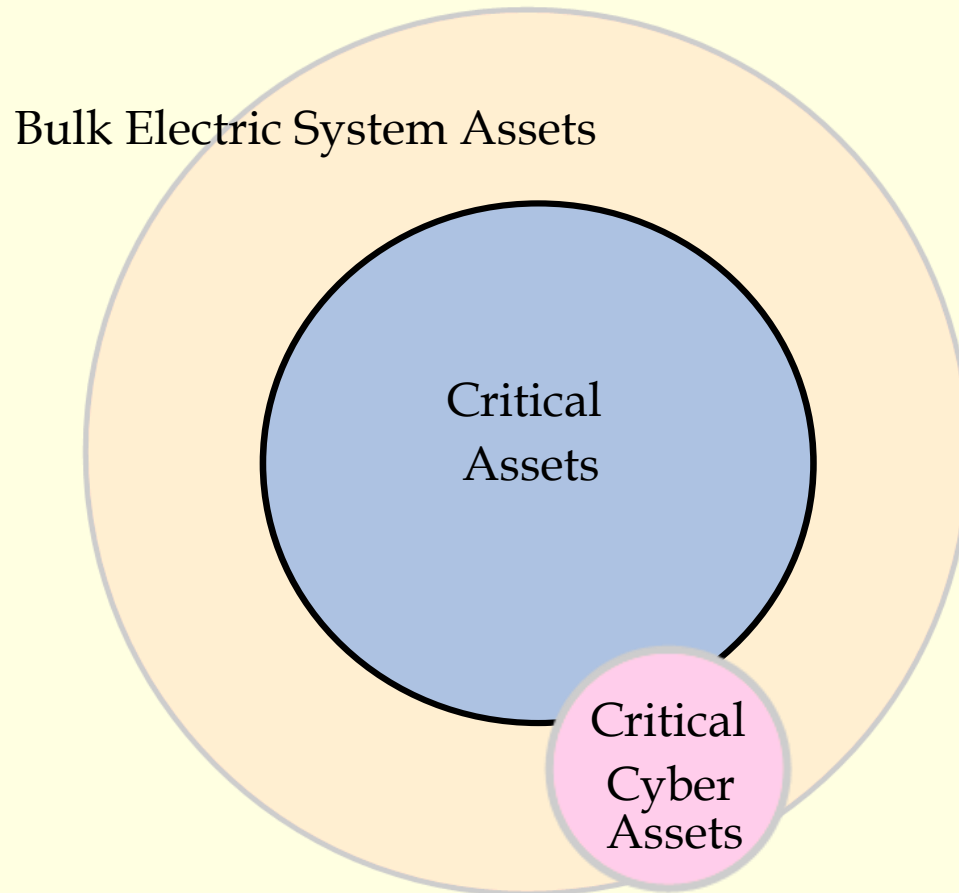
- Full compliance by December 31, 2009
 - Auditably compliant by December 31, 2010
 - **Self-certifications – semi-annual**

Cyber Security Standards (CIP)

- CIP 002
 - Critical Asset Identification
 - **Annual Risk Based Assessment**
 - Critical Cyber Asset Identification
 - **Identification of Critical Cyber Assets associated with Critical Assets**
 - **8 CIP Standards – 200 Procedures**

- **No Critical Cyber Assets**
 - CIP 003 thru CIP 009 don't apply

CIP-002-1 Critical Assets Identification





QUESTIONS?

CyberSecurity Standards: The Generator's Perspective

Adam Menendez, Analyst,
FERC Compliance

Matt Jastram, NERC Specialist,
Power Supply Engineering Systems

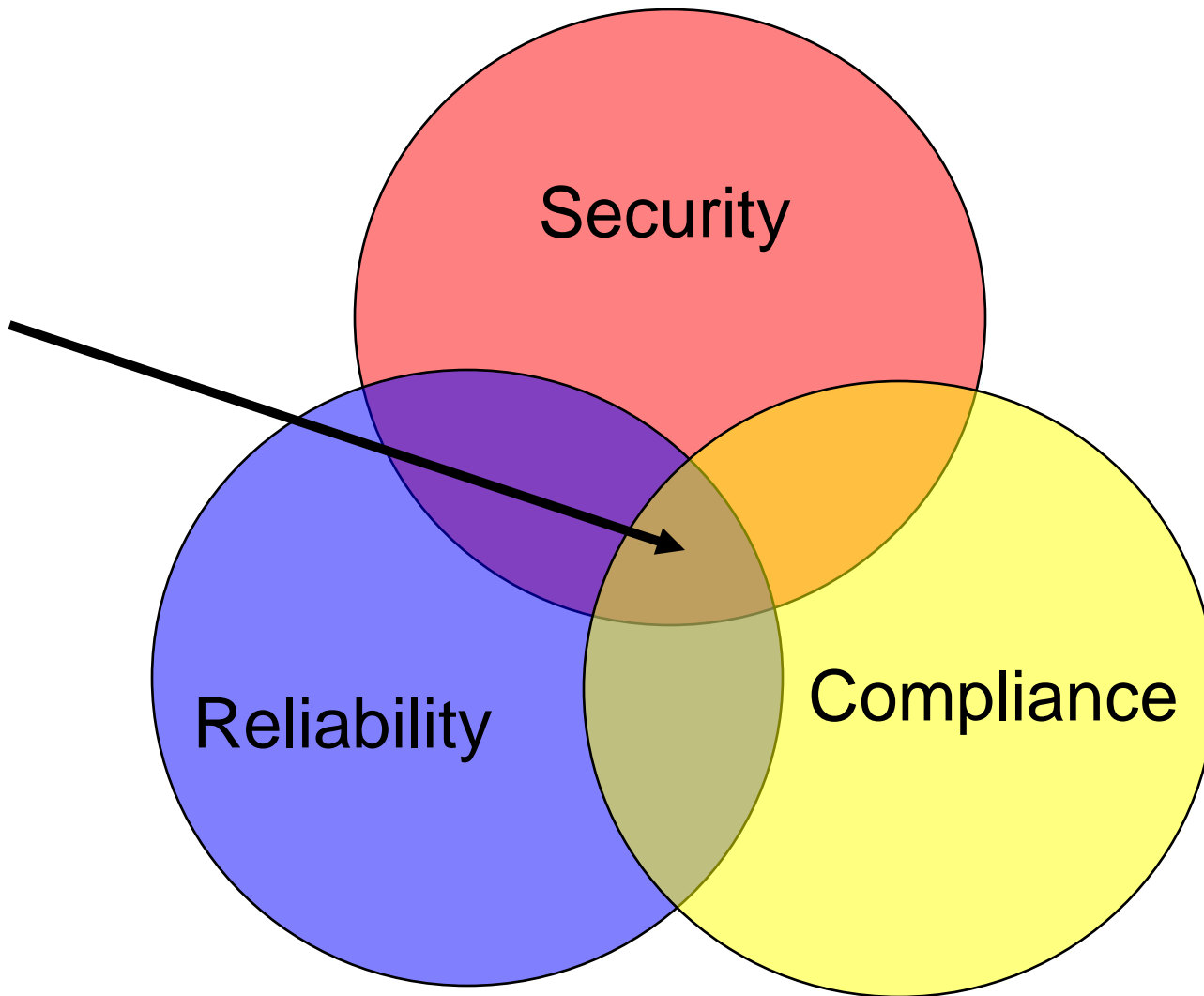
Portland General Electric Company

Key Aspects of the CIP Standards

- “Risk” has a new meaning
 - “Risk” typically = Impact times Probability
 - In FERC’s view of risk, you only look at Impact
 - Don’t consider the likelihood of an event – just the consequences of an event
 - Look at
 - (1) What if the asset were lost, and
 - (2) What if control of the asset was lost to an adversary

Key Aspects of the CIP Standards

- Compliance doesn't always provide Security
- The IT Security industry feels that these standards are a "low bar" for security
- A utility can comply with these standards and still not be secure
- Entities need to find the "sweet spot" for Compliance, Security, and Reliability



With Gratitude to Patrick Miller of WECC

New Versions of CIP Standards

- WECC has a Standard Drafting Team to implement FERC's changes to the Standards
- Version 2 of Standards currently being balloted
 - First set of minor changes
- Version 3 of Standards is next in line
 - Major enhancements to standards

Mounting Political Pressure

- “Aurora” Vulnerability at Idaho National Lab in Spring 2007
- Two House Subcommittees held hearings in Fall 2008 on legislation to increase FERC’s power
- 2009 Hearings on CyberSecurity – House Subcommittee and Senate Commerce Committee
- Latest Season of “24”

How do CIP standards impact a hydro plant?

- NERC Specialist
- Responsible for CIP at PGE generation facilities
- PGE Case Study: Due to PGE's hydro plant facility being capable of Blackstart it fits the profile of a critical asset.

How do CIP standards impact a hydro plant?

- CIP-002-1 requires entities to develop a Critical Asset Identification Methodology
- For methodology development, Hydro plants were integrated as per NERC standards:
 - R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
 - R1.2.4. Systems and facilities critical to system restoration, including Blackstart generators and substations in the electrical path of transmission.
- Identification and annual review

What challenges do CIP standards bring to a hydro plant?

- Our entire Project must follow and meet the Nine NERC CIP standards:
 - 45 Requirements
 - 129 Sub Requirements
 - 25 Annual reviews
- What are Critical Assets and Critical Cyber Assets? (CIP-002-1 R3)
- All measures put in place are to protect both Critical Assets (CAs) and Cyber Critical Assets (CCAs).

What challenges do CIP standards bring to a hydro plant?

- Recent presentation to the affected hydro unit
- Defining and sustaining a new culture of compliance
- Moving instrument and controls personnel out of comfort zone
- Security versus availability
- Facing the reality of change

What challenges do CIP standards bring to a hydro plant?

PGE case study challenges:

- Communication:
 - Keep employees aware
 - Checklist of required actions and documents
 - Provide training
- Monitoring Critical Asset practices for both:
 - Physical access
 - Cyber access

What challenges do CIP standards bring to a hydro plant?

- Developing procedures:
 - Working together to create plant procedures
 - Putting it all on paper
 - A plan for reviewing every step
 - Maintaining living documents



QUESTIONS?

COMPLIANCE PROGRAMS: GOING FORWARD

NWHA Annual Conference, March 19, 2009

Alan Cooke, Project Manager,
Reliability Compliance
Tacoma Power

The Process Continues

- Mandatory standards are here to stay
- Purpose of my presentation – discuss where we go from here. Three areas of emphasis:
 - Continuous compliance
 - Continuous improvement
 - Continuous change

Continuous Compliance

- Compliance is not a discrete event
- All standards require ongoing evidence
- Some standards require annual plan updates
- Moving forward – focus on tools:
 - Systems to manage data, documents and processes
 - Audit tools to monitor compliance

Compliance Monitoring Tools



Pre-Audit Questionnaire and Reliability Standard Audit Worksheet

Registered Entity: *(Must be completed by the Compliance Enforcement Authority)*

NCR Number: *(Must be completed by the Compliance Enforcement Authority)*

Compliance Assessment Method(s): Complaint, Self Reporting, and
Compliance Violation Investigation

Applicable Function(s): All



Compliance Monitoring and Enforcement Program

Reliability Standard Audit Worksheet

RS AW_BAL-STD-002-0

System Restoration Plans

Reliability Standard FERC Approved Date: June, 2007

Applicability: Balancing Authority, Reserve Sharing Group
Within WECC

Continuous Compliance

- Summary: Moving forward, we must continuously monitor and maintain records
- Help is available
 - Numerous vendors
 - Trade associations also involved
 - WECC and NERC sponsor informational sessions
 - Neighboring utilities and other entities

Continuous Improvement

- Areas for improvement moving forward
- Ideal –FERC’s vision of a compliance program:
 - systems and protocols for monitoring, identifying, and correcting possible violations
 - a management culture that encourages compliance among company personnel, and
 - tools and training sufficient to enable employees to comply with Commission requirements

Reference

123 FERC ¶ 61,156
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Joseph T. Kelliher, Chairman;
Sudeen G. Kelly, Marc Spitzer,
Philip D. Moeller, and Jon Wellinghoff.

Enforcement of Statutes, Regulations and Orders

Docket No. PL08-3-000

REVISED POLICY STATEMENT ON ENFORCEMENT

(Issued May 15, 2008)

Continuous Change

- Standards will change
 - New standards under development
 - All standards to be reviewed / revised
 - Standards subject to official interpretations
- Currently 41 projects underway involving 90 standards
- Registered entities, write standards and can drive change



SEARCH NERC.com

Advanced Search GO

- About NERC
- Standards
- Compliance
- Assessments & Trends
- Events Analysis
- Programs

[Failed Standards](#) | [Rejected/Withdrawn SARs and Standards](#) | [Retired Standards](#)

[High-Priority Standards Under Development](#) | [Standard Drafting Team Rosters](#) | [Standard Drafting Team Vacancies](#)

[Standards Under Development Project Status Summary](#) | [Standards Under Development Anticipated Posting Calendar](#)

From this page you can keep track of and link to all proposed reliability standards under development. If you would like to propose a new reliability standard, please download and fill out a [Standard Authorization Request \(SAR\) Form](#).

Reliability Standards - Under Development

Standard Title	Action	Start Date	En
Current Ballots			
Project 2008-09 – Interpretation Of EOP-001-0 R1 By Regional Entity Compliance Managers	Initial Ballot	02/27/09	03
Posted For 30-Day Pre-Ballot Review (Open Ballot Pools)			
Project 2009-10 – Interpretation Of PRC-005-1 R1 By Compliance Monitoring Processes Working Group (CMPWG)	Join Ballot Pool	03/09/09	04
Project 2008-06 – Cyber Security – Order 706	Join Ballot Pool	03/03/09	04

FERC Also Drives Change

- FERC provides guidance to NERC and WECC
- In a recent order FERC called for:
 - Consistency across regions
 - Audits of registered entities' compliance programs
 - Incentives for registered entities for appropriate actions
 - Clear guidance to registered entities

Additional Changes

- NERC Alerts
 - Not standards, but registered entities must respond
 - Three levels of alert
 - Advisory
 - Recommendations to Industry
 - Essential Action
- Other – TBD after the next big outage or security alert? Stay tuned!

Conclusion

- Mandatory standards are here to stay
- We must decide how to respond to the challenges of:
 - Continuous compliance
 - Continuous improvement
 - Continuous change



QUESTIONS?