Western Electricity Coordinating Council

WECC CIPS Update

NW Hydro Operators Regional Forum
Skamania Lodge, Skamania, WA
May 22-23, 2008

Patrick Miller CISA CISSP-ISSAP
WECC Sr. Compliance Engineer, Cyber Security

Overview

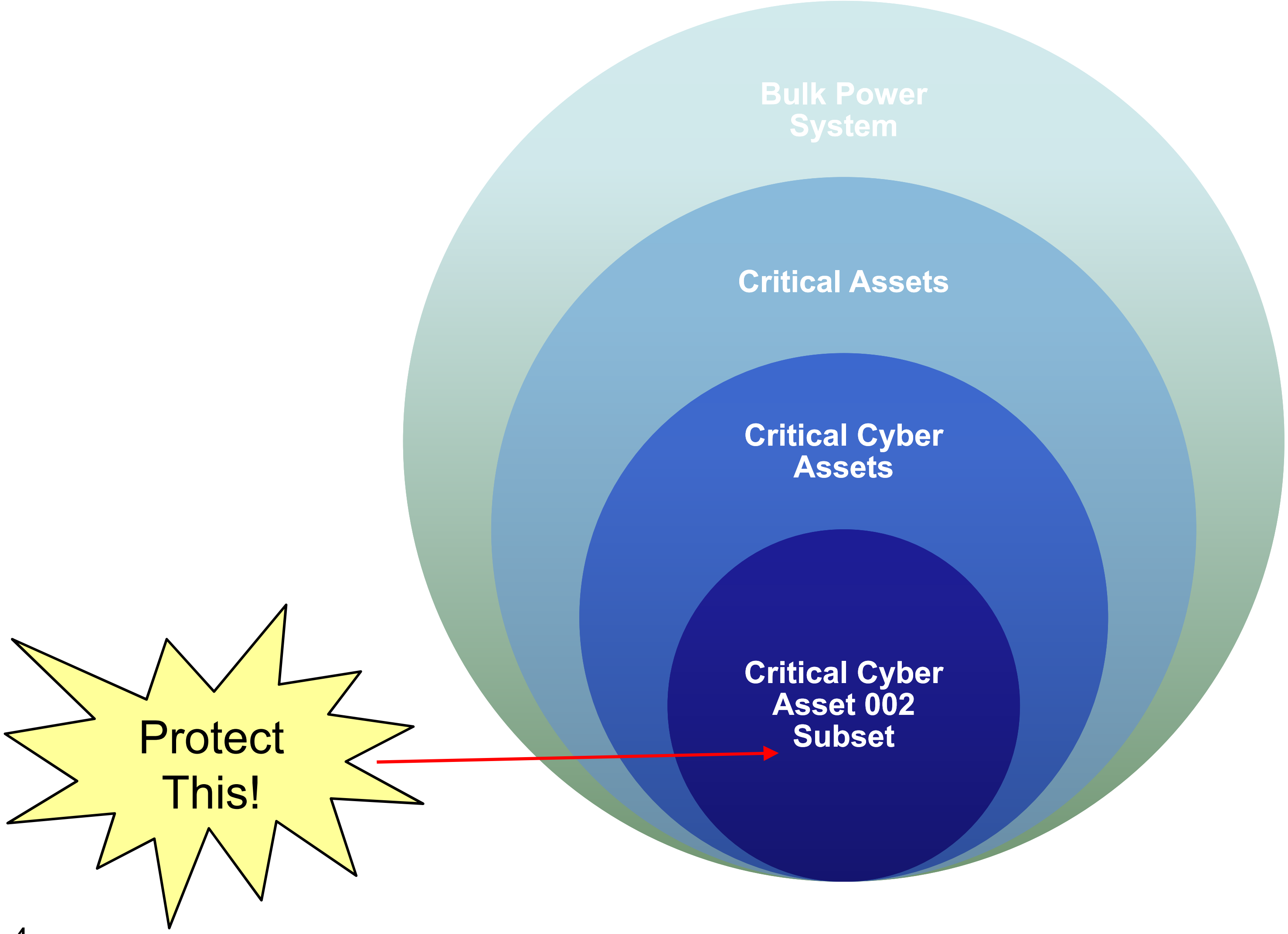
- What is it?
- Why do we need it?
- Where did it come from?
- What are the requirements?
- When do we need to be done?
- What happens if we don’t do it?
- Where is this all headed?

Introduction

- Patrick C. 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

What is CIPS?

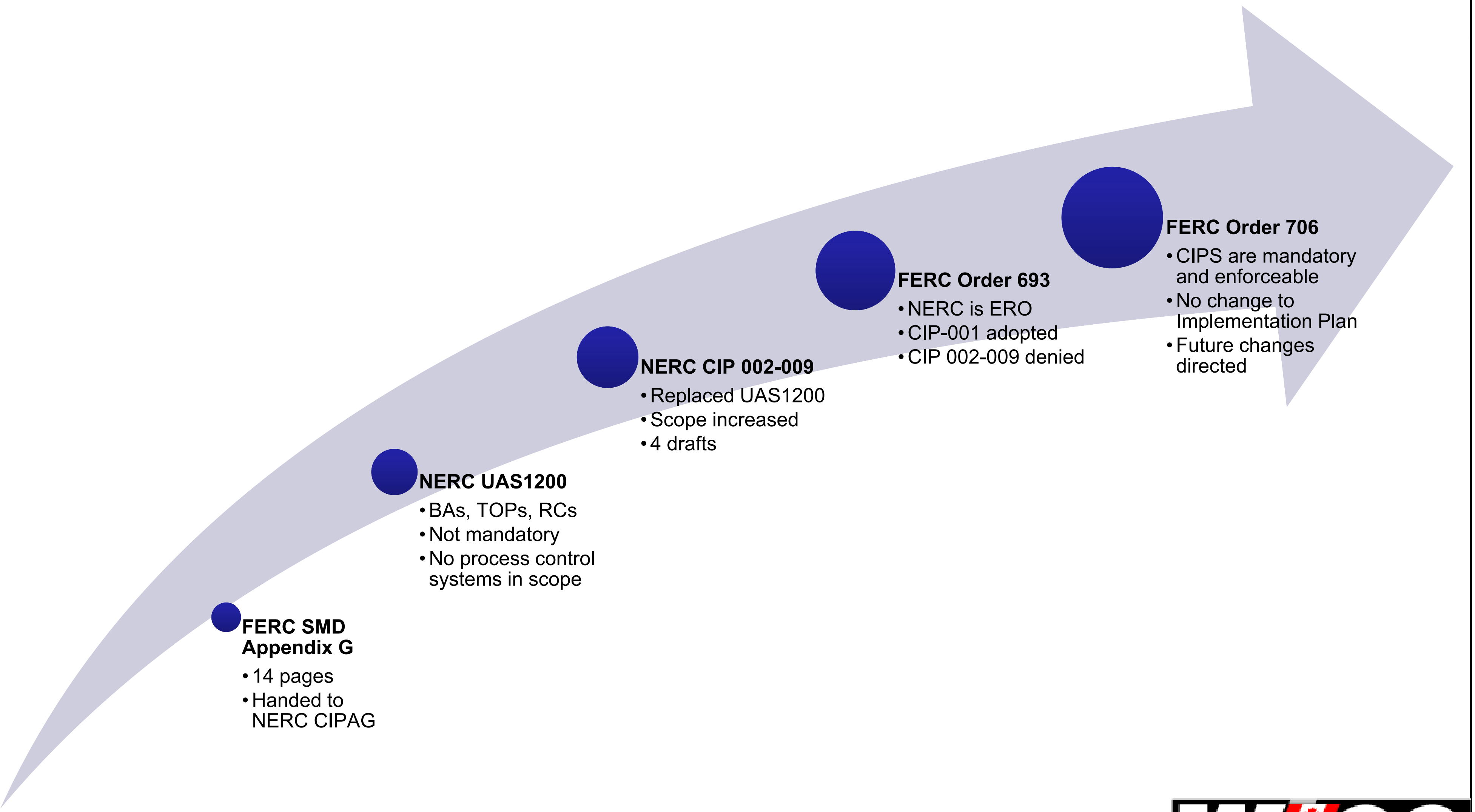
Critical Infrastructure Protection Standards (CIP 002-009)



Why Do We Need CIPS?

- Provides greater reliability through greater security and accountability
- Infrastructure interdependencies are profound
- Target for terrorists and organized crime
- Cyber Warfare [InfoWar]; Zombie armies
- Systems were never designed for security
- Systems are highly inter-connected
- Government and Media attention is growing

CIP History



FERC SMD Appendix G

- 14 pages
- Handed to NERC CIPAG

NERC UAS1200

- BAs, TOPs, RCs
- Not mandatory
- No process control systems in scope

NERC CIP 002-009

- Replaced UAS1200
- Scope increased
- 4 drafts

FERC Order 693

- NERC is ERO
- CIP-001 adopted
- CIP 002-009 denied

FERC Order 706

- CIPS are mandatory and enforceable
- No change to Implementation Plan
- Future changes directed

CIP Present

- CIP-001: Sabotage Reporting

- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter(s)
- CIP-006: Physical Security of CCAs
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for CCAs

- **FAQ and Implementation Plan**

CIP Implementation Plan

- **Table 1:** 13 “Compliant” requirements on 6/30/08
  - Applies to BAs & TOPs that were required to self-certify against the UAS-1200; and RCs
- **Table 2:** 1 “Compliant” requirement on 6/30/08
  - Applies to TSPs; BAs & TOPs that were not required to self-certify against the UAS-1200; NERC and the RROs
- **Table 3:** 1 “Compliant” requirement on 12/31/08
  - Applies to IAs, TOs, TOPs, GOs, GOPs, LSEs; anyone who registered in 2006
- **Table 4:** 1 “Compliant” requirement 12 months after registration date
  - Applies to anyone who registered 2007 and after

Penalties and Sanctions

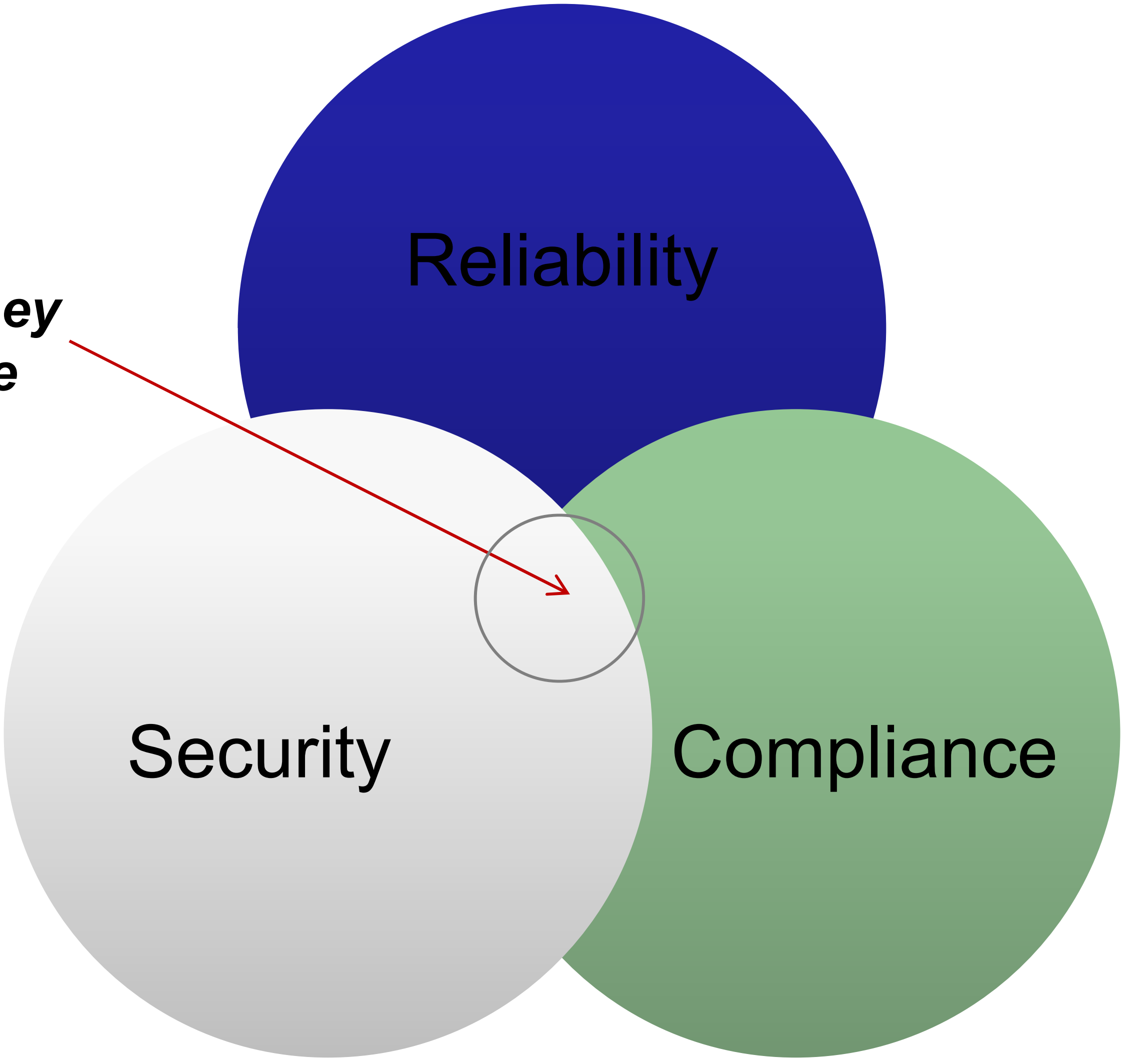
- $1M per day, per violation – plus…
  - Don't forget about Good Utility Practice
- Violation Severity Levels (VSLs)
- Violation Risk Factors (VRFs)
- Mitigating factors
  - Reduce penalties and sanctions
- Aggravating factors
  - Increase penalties and sanctions
  - Any single aggravating factor denies application of any/all mitigating factors
- Can potentially impact rate or license cases

Management Support

- Built into the CIP Standards repeatedly
- Tone at the top is paramount
- Mitigating factor; may reduce fines

- <u>True story</u>: *some have actually asked me to impose penalties and sanctions on their organizations to get management's attention - because they can't (no: I can't do this, even if I tried)*

The Big Picture



Smart money goes here

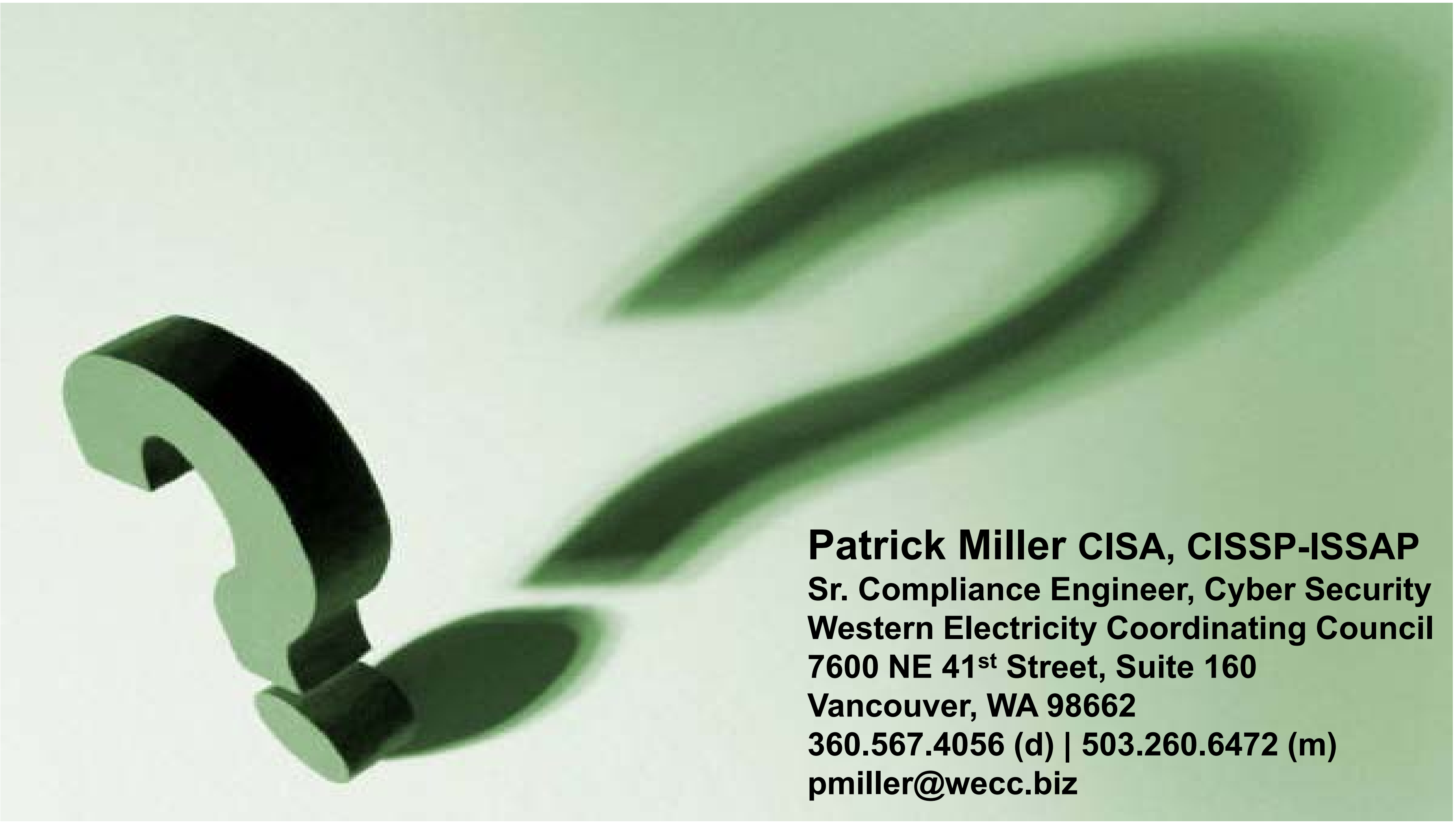
CIP Crystal Ball

- National efforts will influence regulation
  - NIPP, ‘Roadmap’
- NERC
  - New CIPS drafting team is active
  - CIP-010, 011 and 012…
- FERC
  - FERC (and HSC) want a more prescriptive and restrictive standard going forward
  - FISMA/FIPS may be the goal
- A security-related event may accelerate changes or new standard development

Upcoming CIP Events

- WICF: June 9th
  - Portland, OR – Marriott Downtown Waterfront
- WECC CUG: June 10th – 11th
  - Portland, OR – Marriott Downtown Waterfront
- **WECC CIPUG: June 12th – 13th**
  - Portland, OR – Doubletree Lloyd Center
  - Workshop will cover the “first 13” from Table 1
  - Join CIPUG distribution list by sending requests to cnoorda@wecc.biz
- E-Sec NW CIPS Summit: July 23rd – 24th
  - Portland, OR – Doubletree Lloyd Center

Questions?



Patrick Miller CISA, CISSP-ISSAP
Sr. Compliance Engineer, Cyber Security
Western Electricity Coordinating Council
7600 NE 41st Street, Suite 160
Vancouver, WA 98662
360.567.4056 (d) | 503.260.6472 (m)
pmiller@wecc.biz

WECC
Western Electricity Coordinating Council