



Western Electricity Coordinating Council

CIP Standards Brief

NARUC Critical Infrastructure Protection Committee
Hilton Downtown, Portland, OR
July 20, 2008

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

Introduction

- Patrick Miller

- CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM
- 20+ years in IT
- 8+ years in Electric Sector
- Currently employed by WECC
 - Sr. Compliance Engineer, Cyber Security
- I am the WECC CIP Auditor

Overview

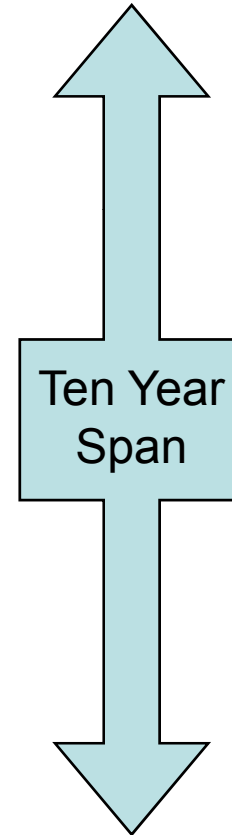
- Current Situation...
- Asset Owner Perspective
 - Creating a new security program
 - Gaining security traction
 - Lessons learned
- Regulatory Perspective
 - WECC 2.0
 - The security “low bar”
 - Auditing the CIPS
- Commission Considerations

CURRENT SITUATION

CIPS Past to Present

- PDD 63
- 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
- FERC Order 706-A

...**05/1998**



...**05/2008**

Influential Factors

- Interdependency studies
- NE Blackout 2003
- “Aurora” DPCD issue
- SANS CIA briefing
- RSA & Ira Winkler
- House Subcommittees
- Chinese Hackers
- Hatch Shutdown
- Project Hydra
- *Hype vs. Reality in the Media*



Geico

ASSET OWNER PERSPECTIVE

Creating a New Security Function

- Management or Technical Practitioner?
- Hire smart; *read: expensive*
 - Certifications
 - Industry experience
 - Regulatory experience
 - Process control security experience
 - Strong communication skills
- Organizational placement matters

Gaining Security Traction

- How do you eat the elephant?
- Event-driven change vs. Insurance model
- Seek first to understand; culture/lexicon
- Baking security into the business process
- Slow methodical approach, invite everyone to the table
- Snake-oil, due-diligence and service availability; *read: expensive*

Security Lessons Learned

- An unskilled operator of any power tool will hurt themselves and those around them
 - Training and staffing are imperative
- Complexity is the enemy
 - Easy to hide things in chaos
- Culture shift – for everyone [self included] – was the hardest part, and it still is...
- Soft-skills mattered more than technical skills
- Merging physical, cyber and control systems is best
- Vendor relationships will make/break all efforts
- “A dime in development is worth a dollar in production”

REGULATORY PERSPECTIVE

WECC, the Start-Up Company

- New era for WECC and all RROs
- Delegation agreement with NERC/ERO
- Compliance/Enforcement roles; what was guidance is now mandatory & enforceable
- Nearly 500 Registered Entities
- Over 2000 Registered Functions
- Dozens of new employees & growing fast
- Still learning (on the job training)

Square One: The Low Bar

- Current standards development process
 - Ambiguous standards, flexibility everywhere
 - The “K” factor
 - Might not fit fast-moving security threats
- Written by the industry for the industry
- One-size fits *some*
- Leaders, ignorance and ostriches
- Competing [and winning] standards
- **All said, they really are helping security**

Auditing the CIP Standards

- Confidential information
 - Highly sensitive information
 - Confidentiality covered by NERC, FERC, CFR
- On-site visit required; WECC can't store the data
- Interpretations are all over the map
 - CIPM WG, RECM and CIPUG are helping
- Very complex Implementation Plan
 - Logistical nightmare

Summary

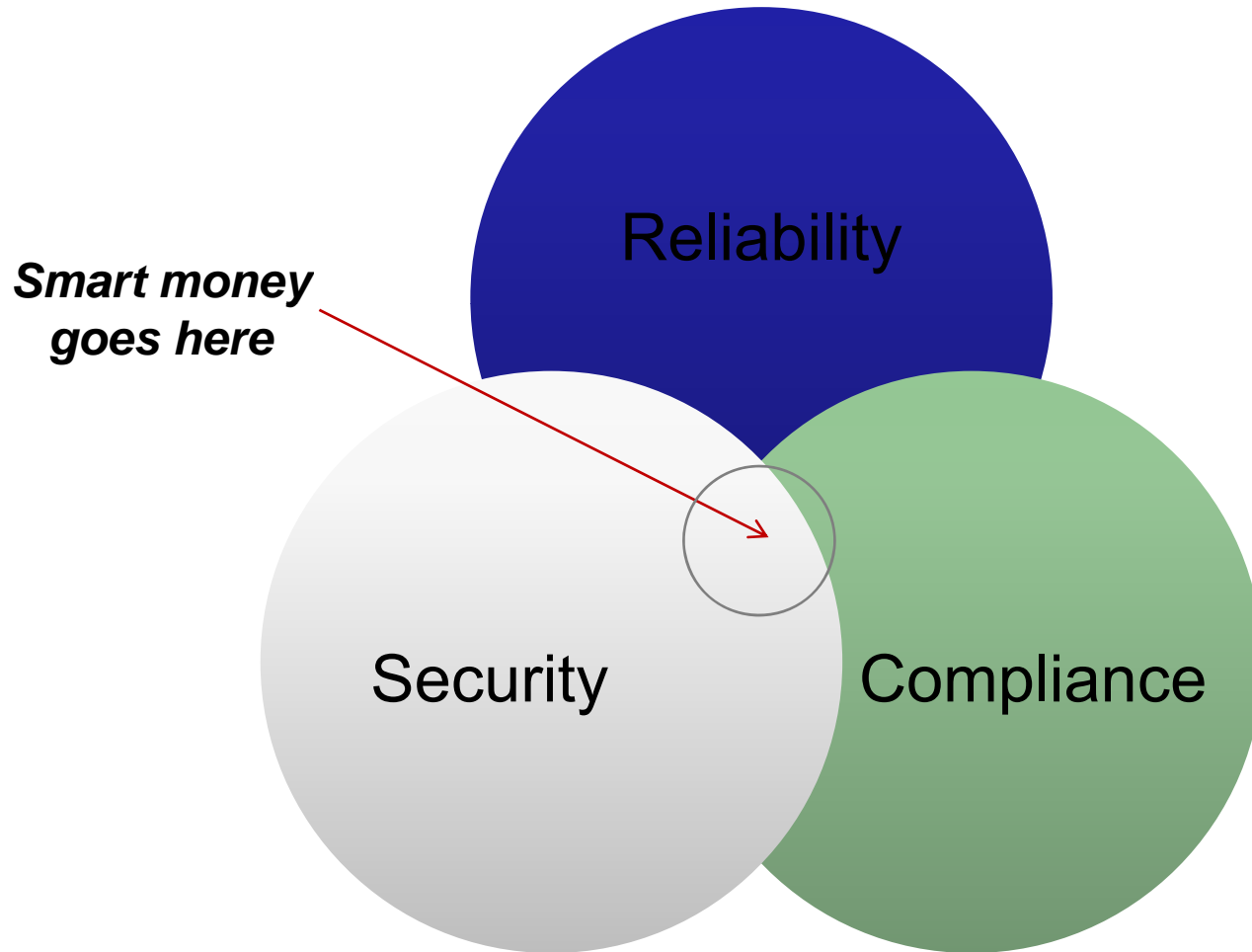
- The CIPS are *very hard* to implement and *very hard* to audit
- Everyone is still learning and growing
 - Even after 10 years, this is still new
- People and technology are hard to find
- Nothing in the CIPS effort is inexpensive
- The industry really wants to be more secure
- This is only the beginning...

COMMISSION CONSIDERATIONS

Prudent Security Expenses

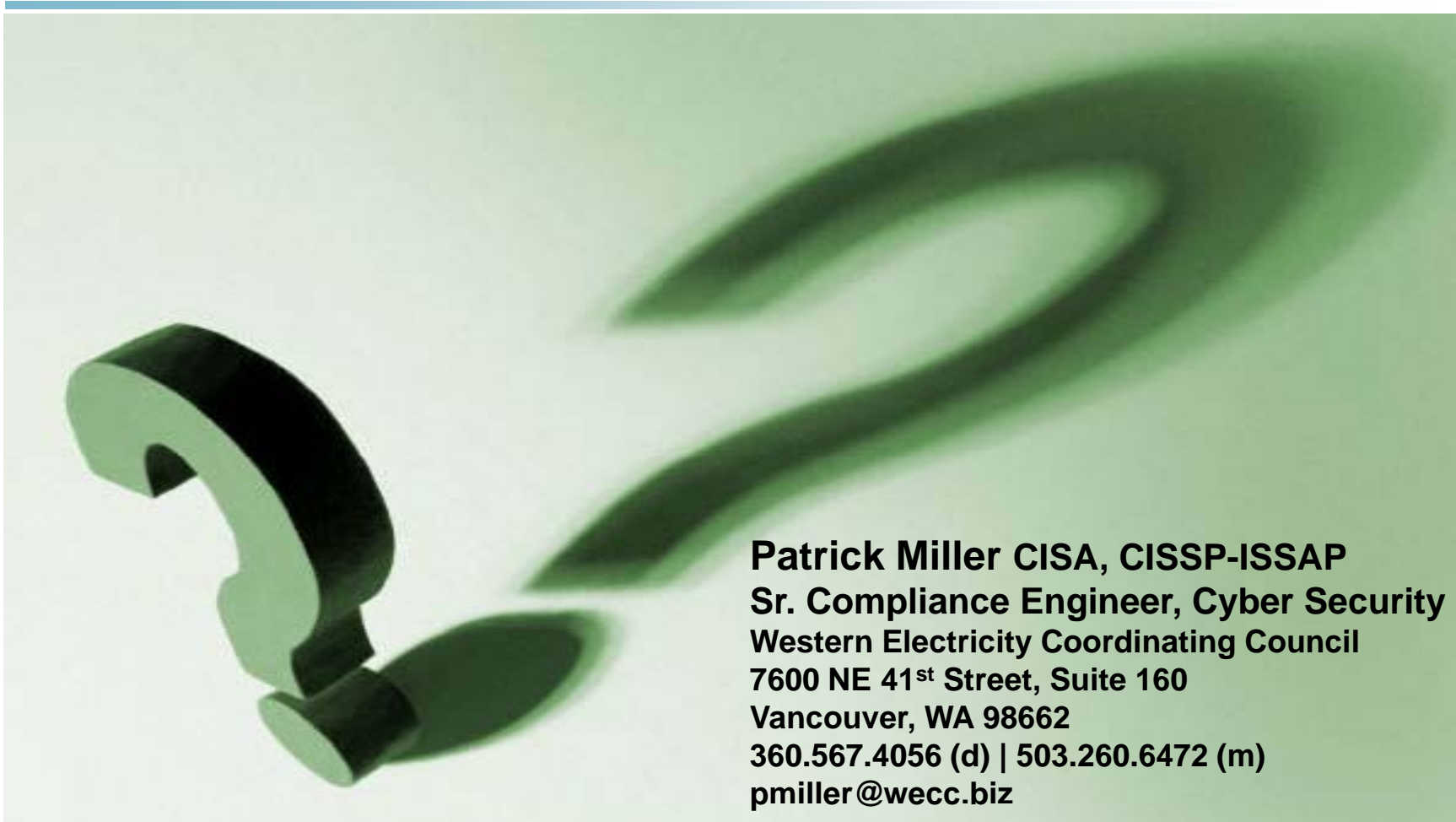
- Security has never been inexpensive
- Security theater is a waste of money
- Security can often be an asset, and may even be recoverable
- Fines and legal fees are not assets
- 80/20 rule still applies; there is no 100%
- People are better at security than technology

The Big Picture



***Smart money
goes here***

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