Preventing a Cyber Attack Through North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Implementation

A successful and proactive implementation of the NERC CIP Standards by Electric Power Organizations will ensure a reduction of risk to the nation's power grid

Introduction

- Eric Cardwell
  - Principal – Commercial Cyber NERC CIP Practice, ICF International
  - CISA, CRISC, & CISSP Certifications
  - Over eighteen years in cyber security
  - Over eleven years in cyber consulting across numerous industries
  - Five years in the Electric Power sector

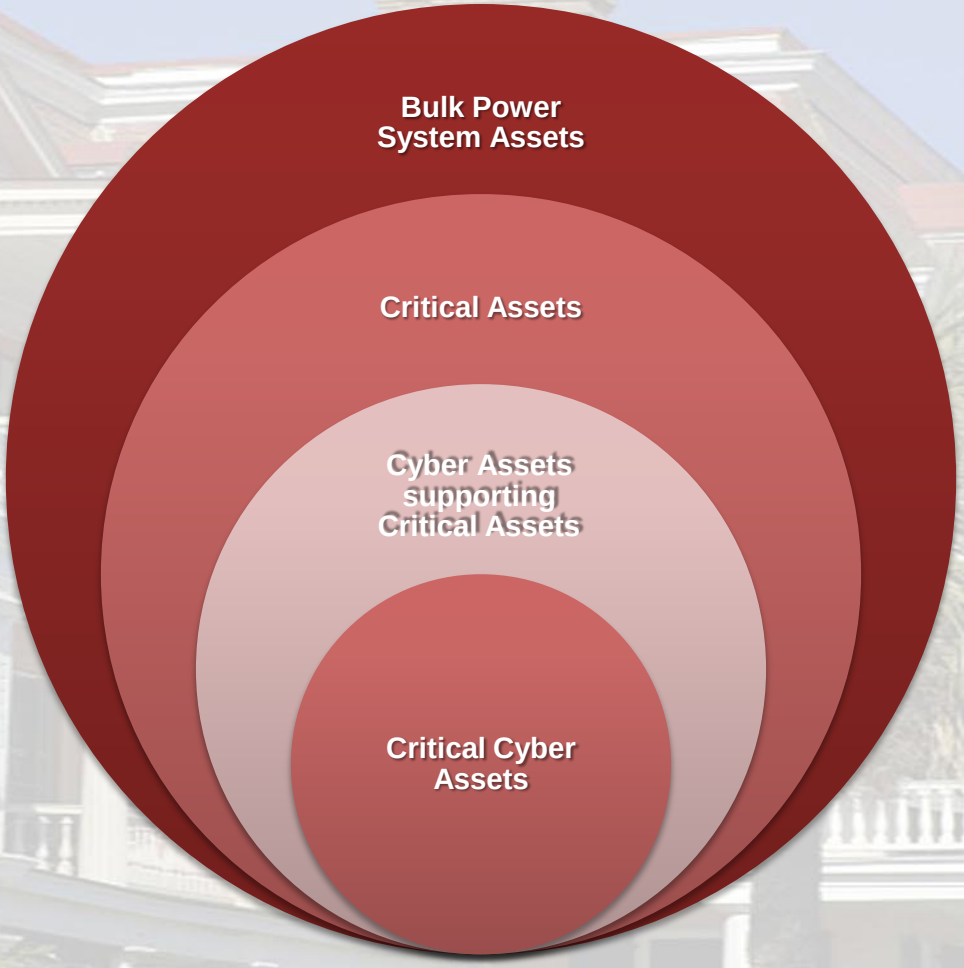
emi sig
EMERGENCY MANAGEMENT ISSUES SPECIAL INTEREST GROUP

Acronyms for Discussion

- CIP = Critical Infrastructure Protection
- NERC = North American Electric Reliability Corporation
- FERC = Federal Energy Regulatory Commission
- BES = Bulk Electric System
- CA = Critical Asset
- CCA = Critical Cyber Asset

emi sig
EMERGENCY MANAGEMENT ISSUES SPECIAL INTEREST GROUP

What Is NERC Trying to Protect?



emi sig
EMERGENCY MANAGEMENT ISSUES SPECIAL INTEREST GROUP

Why Should We Protect It?

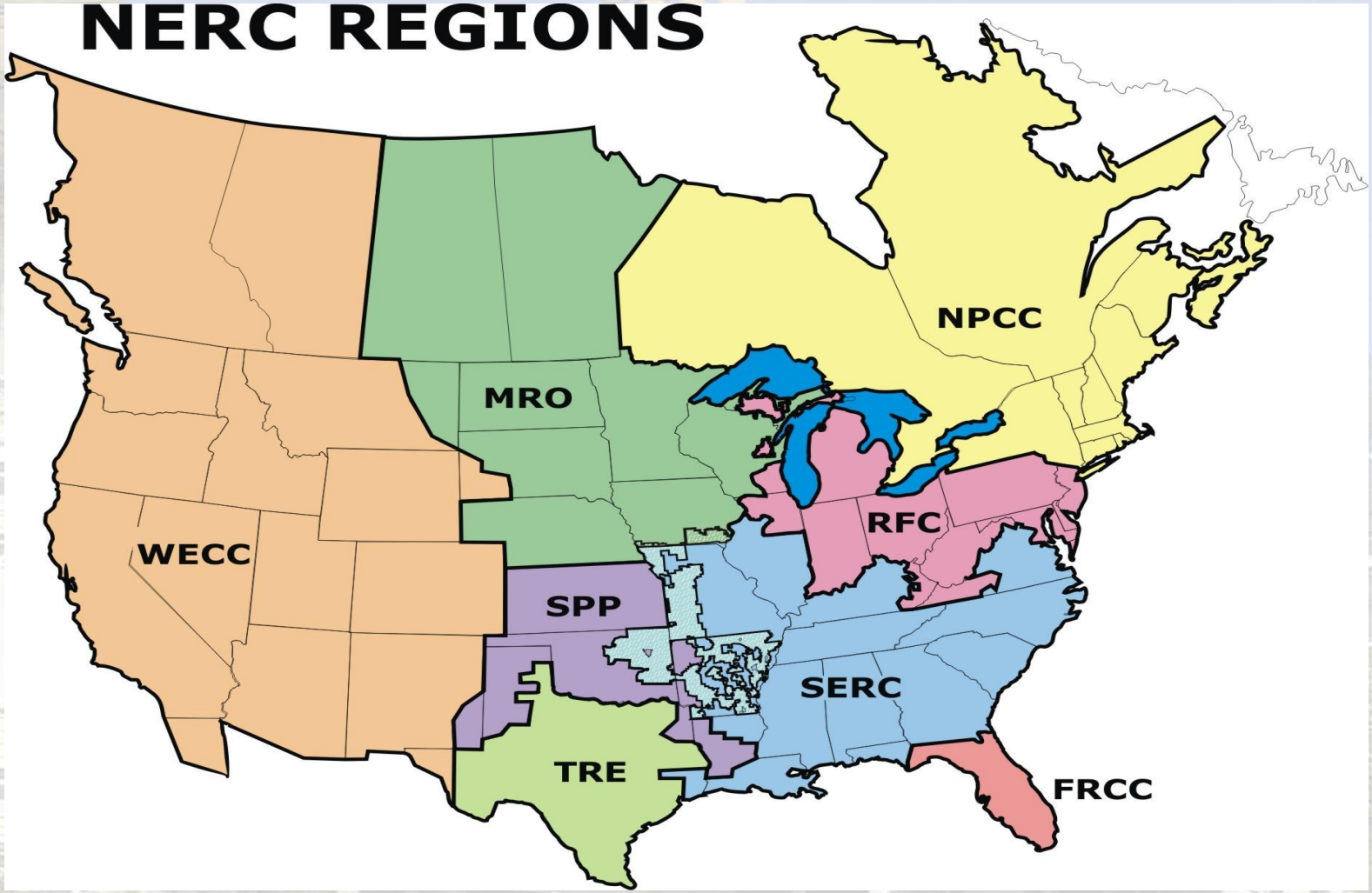
- Feb. 2011 – Night Dragon … targets energy utilities
- Sep. 2010 – Stuxnet … worm targets SCADA systems
- Apr. 2010 - Texas utility's generation system targeted in apparent cyber attack from China - ERCOT
- Jun. 2008 – “Security Hole Exposes Utilities to Internet Attack” – Associated Press
- May 2008 – SCADA vulnerability … control software used by 1/3 of industrial plants. – SC Magazine
- Sep. 2007 – DOE Idaho National Lab video shows the remote destruction of a large SCADA controlled generator

To Whom Does NERC CIP Apply?

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Operator
- Generator Owner
- Load Serving Entity
- Regulatory Entities (WECC, MRO, NPCC, etc…)

emi sig
EMERGENCY MANAGEMENT ISSUES SPECIAL INTEREST GROUP

NERC Auditing Regions



NERC CIP-002 through CIP-009 Timeline

- CIP version 1: July 1, 2008
- CIP version 2: April 1, 2010
- CIP version 3: October 1, 2010
- CIP version 4 – Filed w/ FERC February 2011
- CIP version 5 – in draft

Note: Date range of 1st required compliance to present is only 2 years &10 months

NERC CIP Standards

- 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

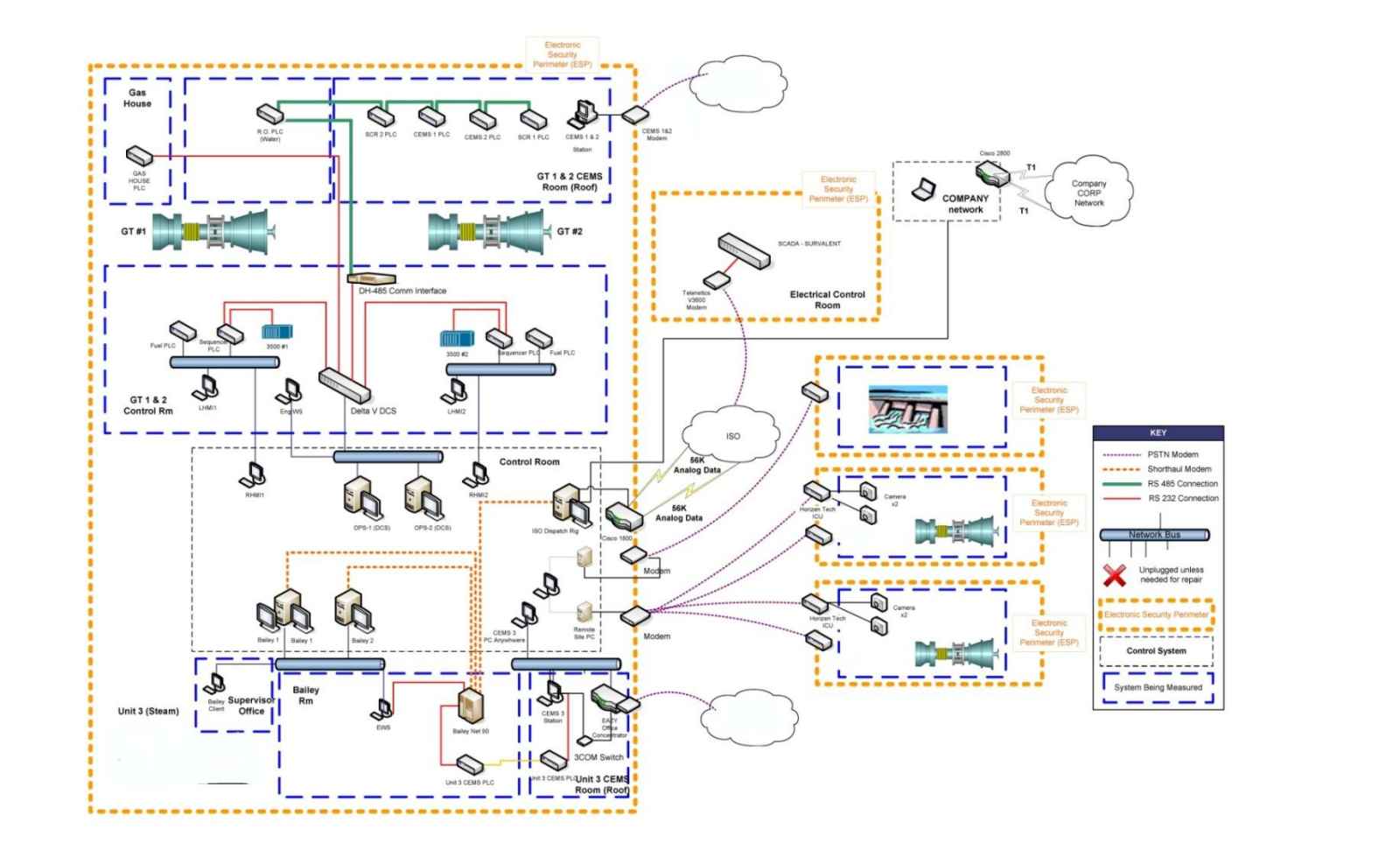
Is NERC CIP Effective?

- Proven security principles can support grid reliability/stability
  - Defense in depth, principle of least privilege, segregation of duties, change/configuration control, deter, detect and respond
- The current CIP standards aren't perfect, but they are a great starting point … currently on Version 3.

General CIP Context

- Applying IT “thought concepts” to operations (control) network environment
  - Policy, Procedure, Access Control, Security Perimeters, Auditing, Change Management
- Focus on Bulk Electric System “Critical Assets”
- Focus on “Critical Cyber Assets”
- Focus on “routable protocol” communications
- Process and documentation centric
- Balance of accountability and security

CIP-005 Example ESP Diagram

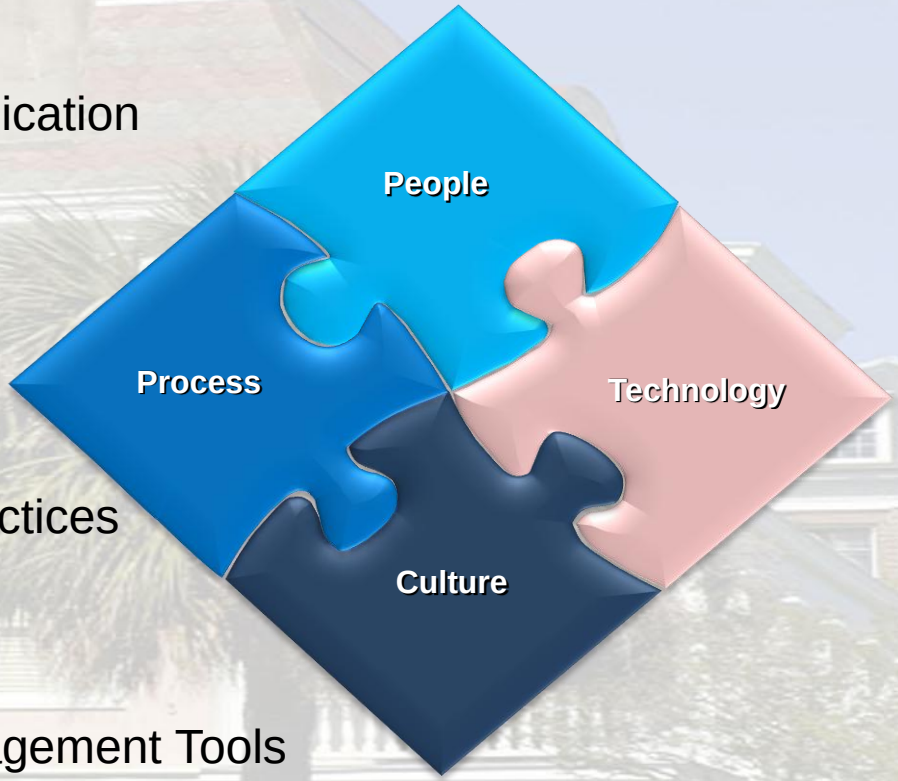


With CIP, Timing Is Everything

- Annual
- Quarterly
- Calendar days vs. business days
- Frequency “bookends”
  - Must be performed prior to Compliance date (per your respective implementation plan)

CIP Compliance Elements

- People
  - Leadership
  - Tone at the Top
  - Established Lines of Communication
- Culture
  - Vision, Mission, and Values
  - Organizational Character
  - Code of Conduct
  - Relationships / Dynamics
- Process
  - Policies, Procedures, and Practices
  - Accountability
  - Control Framework
- Technology
  - Monitoring and Security Management Tools
  - Resources and Training



Technology Issues in the Industry

- Control Systems are not as isolated as plant personnel believe
- Closing up holes in the Electronic Security Perimeters requires significant coordination with Vendors for remote support, monitoring and upgrades
- Mitigating controls often thwarted by lack of copper or fiber capacity between locations … expensive upgrades to pull new cable
- Generation facilities far less likely to install updates after plant fit-up compared to Transmission or other responsible entities
- Control System Vendors recognize the security concerns and are vetting patches to applications on supported versions of OS
- Excuse of "vendor won't support patch" is going away
- Requires software upgrades to supported versions of software

emi sig
EMERGENCY MANAGEMENT ISSUES SPECIAL INTEREST GROUP

Current and Future Challenges

- Not enough qualified security professionals are available
- Very complex range of skills needed
- New talent is being trained
  - Academic vs. in-the-field experience
  - Training options are limited and/or questionable
- Technical training available, but little or none for soft skills

Organizations Should Be Proactive

- Risk-based mock audits (internal and external)
- Cyber vulnerability assessments
- Incident response exercises
- Disaster recovery exercises
- Emergency management scenarios

emi sig
EMERGENCY MANAGEMENT ISSUES
SPECIAL INTEREST GROUP

Questions