

The “Cyber” House Rules: What Regulators Need To Know About Cyber Security

10 Things To Consider

Jim Fama
Executive Director, Energy Delivery
Edison Electric Institute

NARUC

Chicago, IL

November 17, 2009



1: Distinguish Between Bulk Power And Distribution System Cyber Security

- Bulk Power System (BPS)
 - 8 NERC Critical Infrastructure Protection (CIP) Standards.
- Distribution System
 - State public service commission rules and regulations.
 - National Institute for Standards and Technology (NIST) Interoperability Standards.

2: Bulk Power System: Ask About Compliance With NERC CIP Standards

- NERC audits all utilities for compliance with 8 CIP Standards:

- Asset Identification
- Security Controls
- Personnel & Training
- Security Perimeters
- Physical Security
- Security Management
- Incident Reporting
- Recovery Plans

3: Participate In NIST Coordination Of Interoperability Standards Development

- NIST is coordinating (not developing) interoperability standards to be filed with FERC.
- Most standards pertain to distribution.
- A very important part—NIST will develop framework for testing and certification of devices and software.

4: Participate In Organizations That Develop Standards and Protocols



5: Participate In FERC Rulemaking To Approve Interoperability Standards

- Ultimately, NIST will file interoperability standards with FERC.
- Before adopting the standards, FERC needs to be sure they adequately provide for cyber security.

6: Look At Current State Commission Requirements

- Commission Rules and Policies
 - Up to date?
 - Best practices of state commissions.
- Examples:
 - Cyber security plan in place (PA)
 - Commission analysis of security (NY)
 - NERC CIP standards (MI)

7: For Smart Grid Matching Fund Projects, Look At Cyber Protection Measures

- Energy Independence and Security Act of 2007 (EISA)
 - Smart Grid Matching Program
 - Functions must include:
 - **“The ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cyber-security threats and terrorism...”**

8: Keep In Mind That Federal Cyber Security Legislation Is Possible

- 5 pending bills that would give Federal government authority to order changes in utility operations in the face of a security emergency.
 - **WHO** – Which govt. entity gets the authority?
 - **WHAT** – What is the scope of this authority?
 - **WHEN** – What triggers use of this authority?
 - **HOW** – Is there consultation with industry?
- Broad coalition of industry stakeholders (including EEI and NARUC) have developed legislative framework.

9: Distinguish Between Utility Operations And National Defense / Law Enforcement

- Cyber secure utility operations is the domain of operating utilities.
- Defending against nation-state cyber attacks and cyber terrorism are national defense and law enforcement matters.
- Effective cyber security takes utility / federal agency (DHS, etc.) partnership.

10: “Case By Case” Approach: Check In With Your Utility

- Many cyber issues in process, e.g.
 - NERC CIP standards enforcement is evolving.
 - Finalization / implementation of NIST interoperability standards is a ways off.
 - Smart grid projects are at various stages of implementation.
- In the meantime, utilities are dealing with cyber security every day.