



Edison Electric Institute

Power by AssociationSM

When Prevention and
Preparation May Not be Enough:
**Resilience and Recovery for the
Electricity Sub-Sector**

GMD Workshop

David Batz,
Director of Cyber and Infrastructure Security
April 8, 2015

Bulk Electric System Resilience

- Engineered for fault tolerance
- In the face of failure scenario:
 - Respond
 - Restore
 - Recover

Regulations

Necessary but
not sufficient

Bulk Electric System Resilience

EEI

Spare Transformer
Equipment Program

STEPTM

- 500-230 kV
- 345-161 kV
- 345-138 kV
- 345-115 kV
- 230-138 kV
- 230-115 kV
- 230-069 kV
- 138-069 kV

EEI

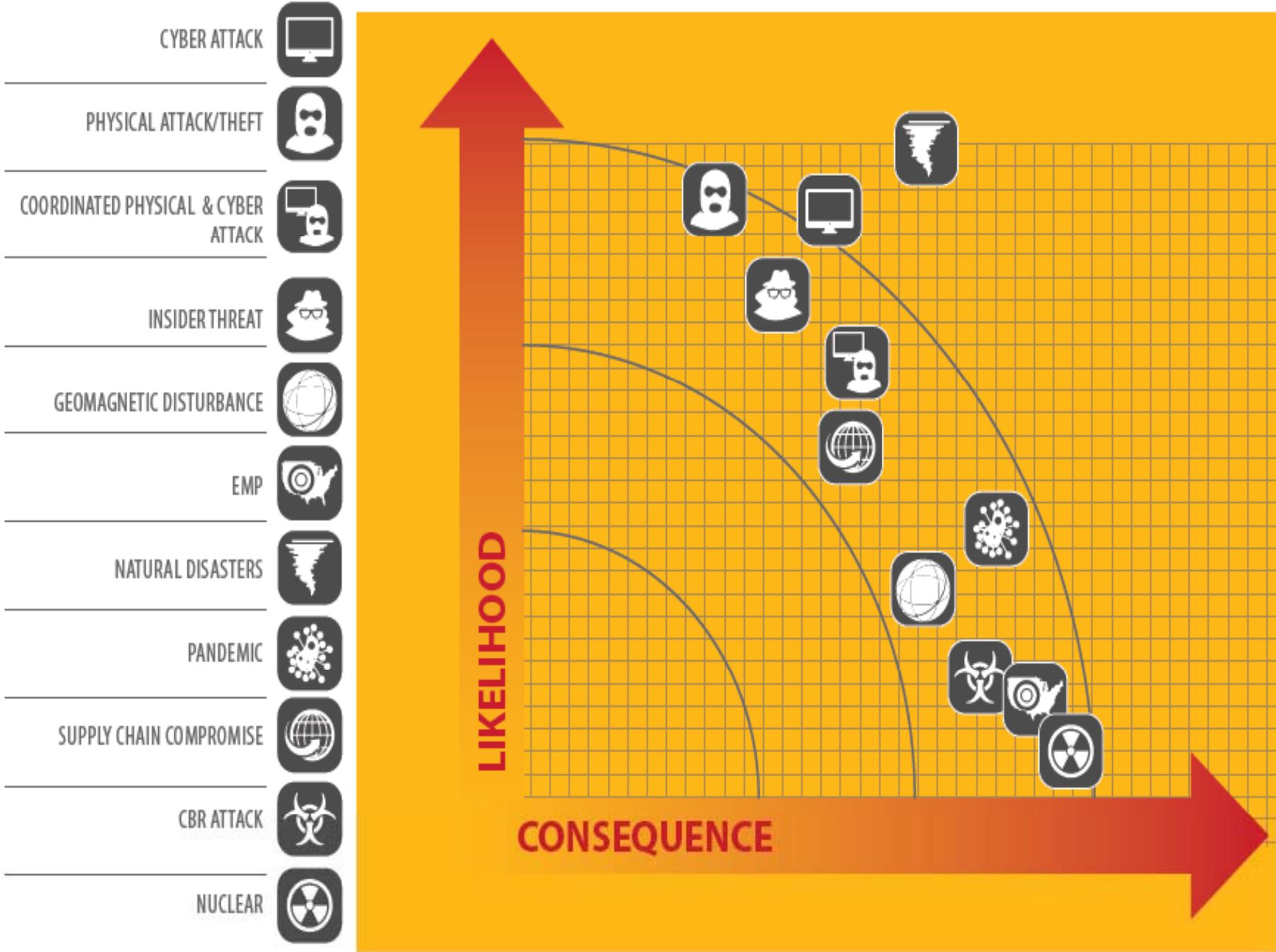
International Resilience

SPARE CONNECT

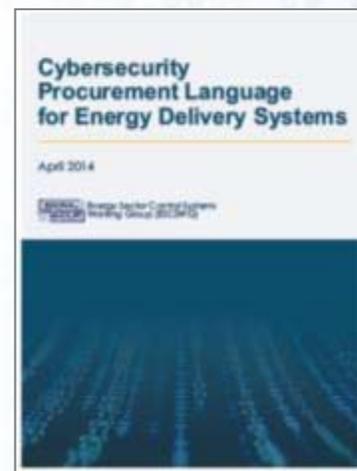
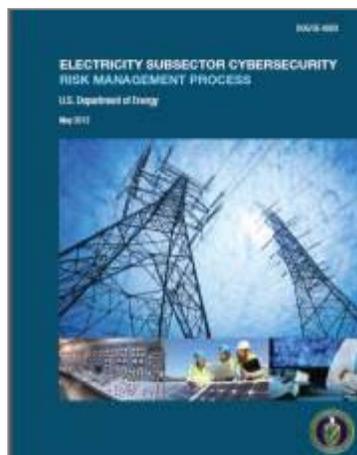
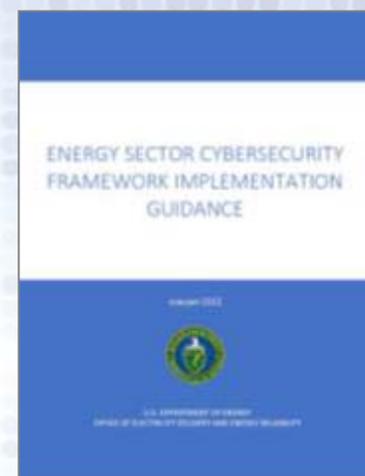
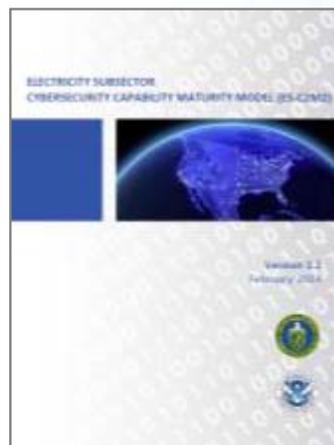
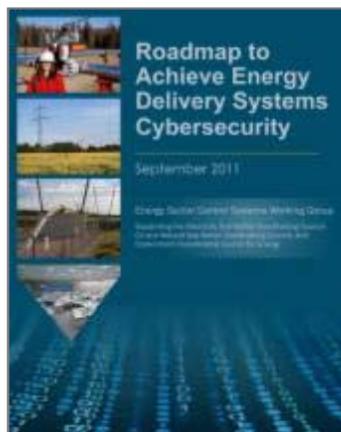
- Voluntary Program
- Provides access to transmission and generation step-up (GSU) transformers and related equipment, including bushings, fans, and auxiliary components.
- An Online tool to
 - Communicate equipment needs
 - Identify points of contact for equipment
- Utility-to-Utility arrangements are made offline



THREAT LANDSCAPE: ELECTRIC UTILITY SECTOR



Examples of Energy Sector Specific Cybersecurity Collaborative Efforts



Supply Chain Cybersecurity Risk

- Unintentional and intentional threats
 - Threat vectors - malicious code, counterfeit parts, defective parts
 - Impact – systems that don't do what they are supposed to do; systems that do something they are NOT supposed to do
- Vulnerabilities
- Potential consequences
 - Business disruptions
 - Electric grid reliability issues

Approaches to Managing Supply Chain Cybersecurity Risk

Complexity
Responsibility

People

Multi-disciplinary teams
Vendor collaboration

Existing Infrastructure
Regulatory Environment

Process

Risk-based prioritization
Procurement

Functionality v. Security
Transparency
Diversity

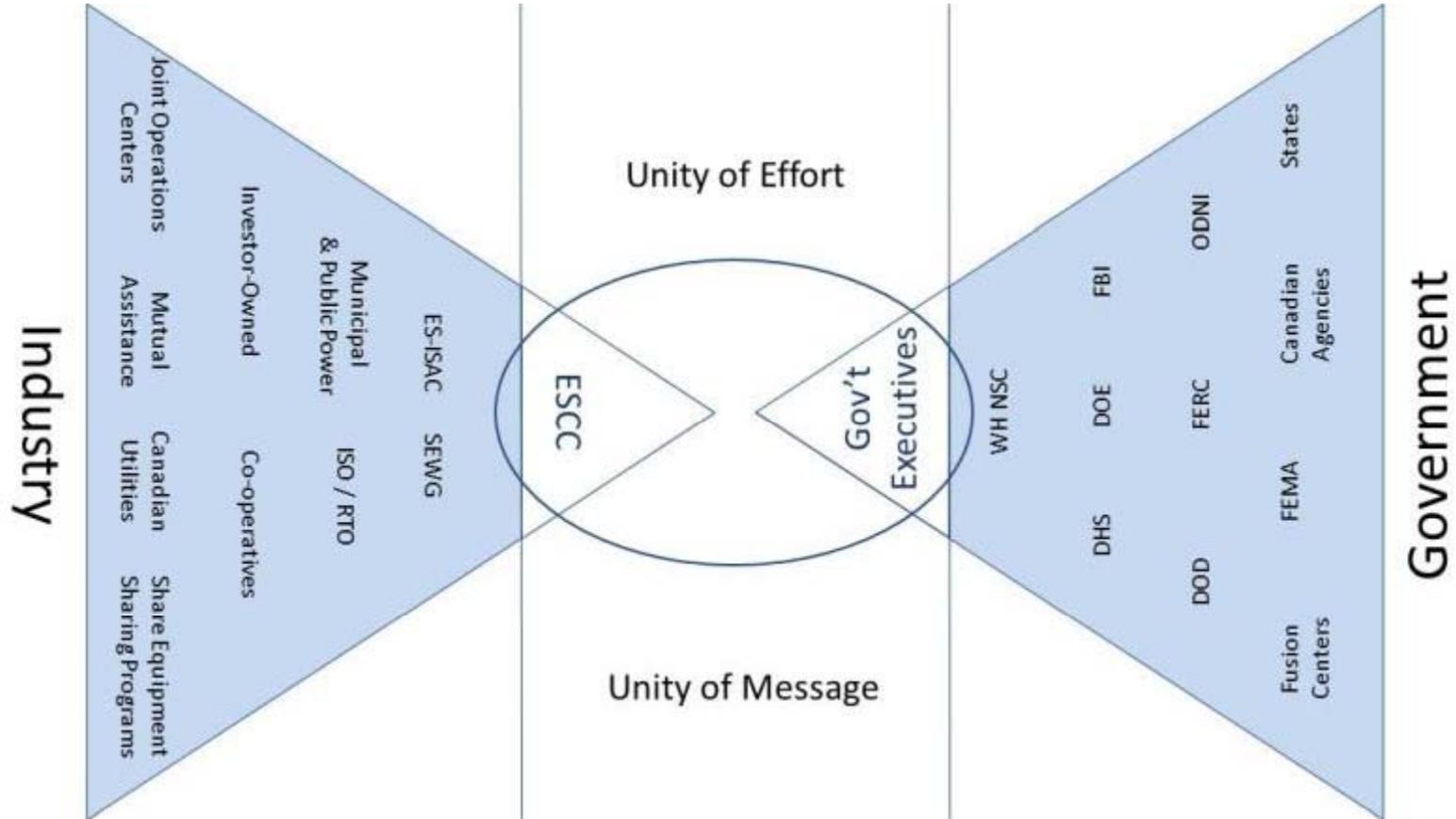
Technology

Enterprise-wide policy
Code analysis and audits
Industry collaboration

EEI Principles for Managing Supply Chain Cybersecurity Risk

- Managing risk is a shared responsibility
- Supply chain cybersecurity requires cross-functional cooperation
- Risk management is a continuous process
- Secure Manufacturing and Development Practices are Essential
- Cybersecurity must be built into systems

Industry-Government Coordination



ESCC Organizational Structure



ESCC Committee Structure

