



Edison Electric Institute

Power by AssociationSM

Cyber Security Policy and Critical Infrastructure Protection: Protecting Our Key Electrical Assets

David Batz
Director – Cyber and Infrastructure Security
Mid-America Regulatory Conference

June 3, 2014

Recent Media Reports...

THE WALL STREET JOURNAL.

**Assault on California Power Station
Raises Alarm on Potential for
Terrorism**



**Sniper Attack On Calif. Power Station
Raises Terrorism Fears**

Bloomberg

**Electric-Grid Attack Fuels Sniper-
Versus-Hacker Debate**

The New York Times

**Power Grid Preparedness Falls Short,
Report Says**

 **USA TODAY**

**Concern Over Power Grid Security
Mounts in Congress**



**High-Powered Attack On PG&E
Substation Raises Concerns About
Combined Threats to Grid**

THE WALL STREET JOURNAL.

**U.S. Risks National Blackout from
Small-Scale Attack**

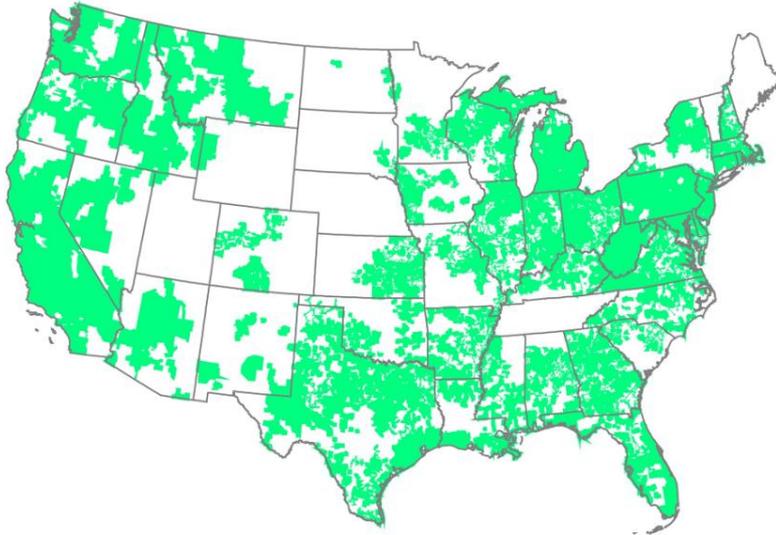
National Journal

**How Safe and Reliable is America's
Electric Grid?**



Spare Transformer Equipment Program - 2006

SpareConnect - 2014



SPARE CONNECT

SpareConnect offers an online tool to communicate a utility's bulk power system equipment needs and provides point of contact information for people and equipment across the North American electric utility industry for specific equipment categories and classes.

EI Threat Scenario Project (2011)

 Edison Electric
Institute
Power by Association

EI Threat Scenario Project

Resiliency Self-Assessment User's Guide

Prepared by: Edison Electric Institute

March 2012



- Coordinated Cyber Attack
- Advanced Persistent Threat
- Disruption of Voice and Data Services
- Coordinated Physical and Cyber Attack
- Insider Sabotage
- Pandemic
- Supply Chain Disruption or Compromise
- Catastrophic Human Error
- Intentional Electromagnetic Interference
- Distributed Denial of Service

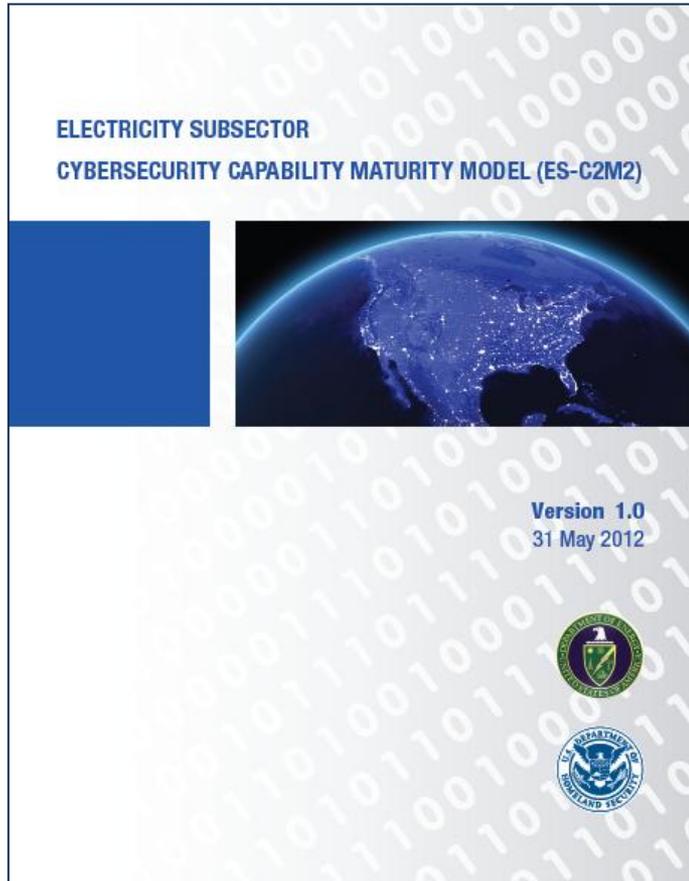
Self-assessments based on threats and mitigation measures.



Executive Order 13636 – NIST Cyber Security Framework



DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model



Domains in maturity model in which utilities are evaluated:

1. Asset, Change, and Configuration Management (ASSET)
2. Workforce Management (WORKFORCE)
3. Identity and Access Management (ACCESS)
4. Risk Management (RISK)
5. Supply Chain and External Dependencies Management (DEPENDENCIES)
6. Threat and Vulnerability Management (THREAT)
7. Event and Incident Response, Continuity of Operations (RESPONSE)
8. Situational Awareness (SITUATION)
9. Information Sharing and Communications (SHARING)
10. Cybersecurity Program Management (CYBER)