Developments in Cybersecurity Compliance

David W. Opderbeck, Professor of Law – Seton Hall University Law School

David Coher, Director, Compliance and Safety – Southern California Edison Company

SETON HALL | LAW

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Regulatory Update

David W. Opderbeck
Professor of Law
Seton Hall University Law School

SETON HALL | LAW

Cybersecurity Regulatory Framework

- Specific ad hoc rules and guidance documents for some regulated industries:
  - Healthcare: HIPAA
  - Financial Services
    - GLBA
    - SEC Guidance
    - FINRA Guidance
  - Energy Sector
    - DOE Guidance
    - NERC Standards
- But no overarching, coordinated framework

Cybersecurity Regulatory Framework

- A vexing problem: safeguarding critical infrastructure and vulnerable people while maintaining the unique open forum of the Internet
- The solution?
  "Regulate cyberspace." -- Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency" (December 2008)
  - ***Really?***

Cybersecurity Regulatory Framework

- Cybersecurity Act of 2009 (not passed)
  - The "Kill Switch?": The President ... "May declare a cybersecurity emergency and ... may order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security ... "

Cybersecurity Regulatory Framework

- Cybersecurity Act of 2010: Emergency Measures (not passed)
  - The President would promulgate, after public notice and comment, a set of cyber emergency response plans.
  - The President would retain the authority to "declare a cybersecurity emergency," which would trigger implementation of the emergency response plans.
  - Within forty-eight hours after declaring a cybersecurity emergency, the President would be required to report to Congress, with supplemental reports every thirty days until the emergency declaration is removed.

Cybersecurity Regulatory Framework

- Protecting Cyberspace as a National Asset Act of 2010: Emergency Measures (not passed)
  - National cyber emergency" could be declared "if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure."

Cybersecurity Regulatory Framework

- Protecting Cyberspace as a National Asset Act of 2010: Emergency Measures (not passed)
  - "Risk": "the potential for an unwanted outcome resulting from an incident, as determined by the *likelihood of the occurrence of the incident* and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident."
  - "Incident": "an occurrence that actually or imminently jeopardizes" the security of information infrastructure or the information within information infrastructure, as well as any occurrence that "*constitutes a violation of security policies, security procedures, or acceptable use policies applicable to information infrastructure.*"

Cybersecurity Regulatory Framework

- Cybersecurity and Internet Freedom Act of 2011: Emergency Measures (not passed)
  - National cyber emergency" could be declared "if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure."

Cybersecurity Regulatory Framework

- Cybersecurity Act of 2012: Compliance Incentives (not passed)
  - Establish "a multi-agency National Cybersecurity Council"
  - "[a]llow private industry groups to develop and recommend to the council voluntary cybersecurity practices to mitigate identified cyber risks”
  - "[a]llow owners of critical infrastructure to participate in a voluntary cybersecurity program.“
  - voluntary program would involve certification process and would provide "benefits including liability protections, expedited security clearances, and priority assistance on cyber issues."

Cybersecurity Regulatory Framework

- Critical Information Infrastructure: Executive Order 13636 (2013) and the NIST Framework

Cybersecurity Regulatory Framework

- Cybersecurity Act of 2015: Information Sharing (passed)
  - Facilitates sharing of cyber threat information among private sector organizations and with the government
  - Liability protections if information is shared
  - No common compliance framework

Cybersecurity Regulatory Framework

- Other "regulatory" frameworks:
  - FTC Enforcement of Privacy Policies
  - State Data Breach Notification and other State Privacy Laws
  - Consumer and Other Litigation Arising from Data Breaches

Current Application Example: Energy Sector

David Coher
Director, Compliance and Safety
Southern California Edison Company

Disclaimer

The opinions expressed in this presentation are my own and do not necessarily represent the positions, strategies or opinions of Southern California Edison, its parent company Edison International, or any of their affiliates.

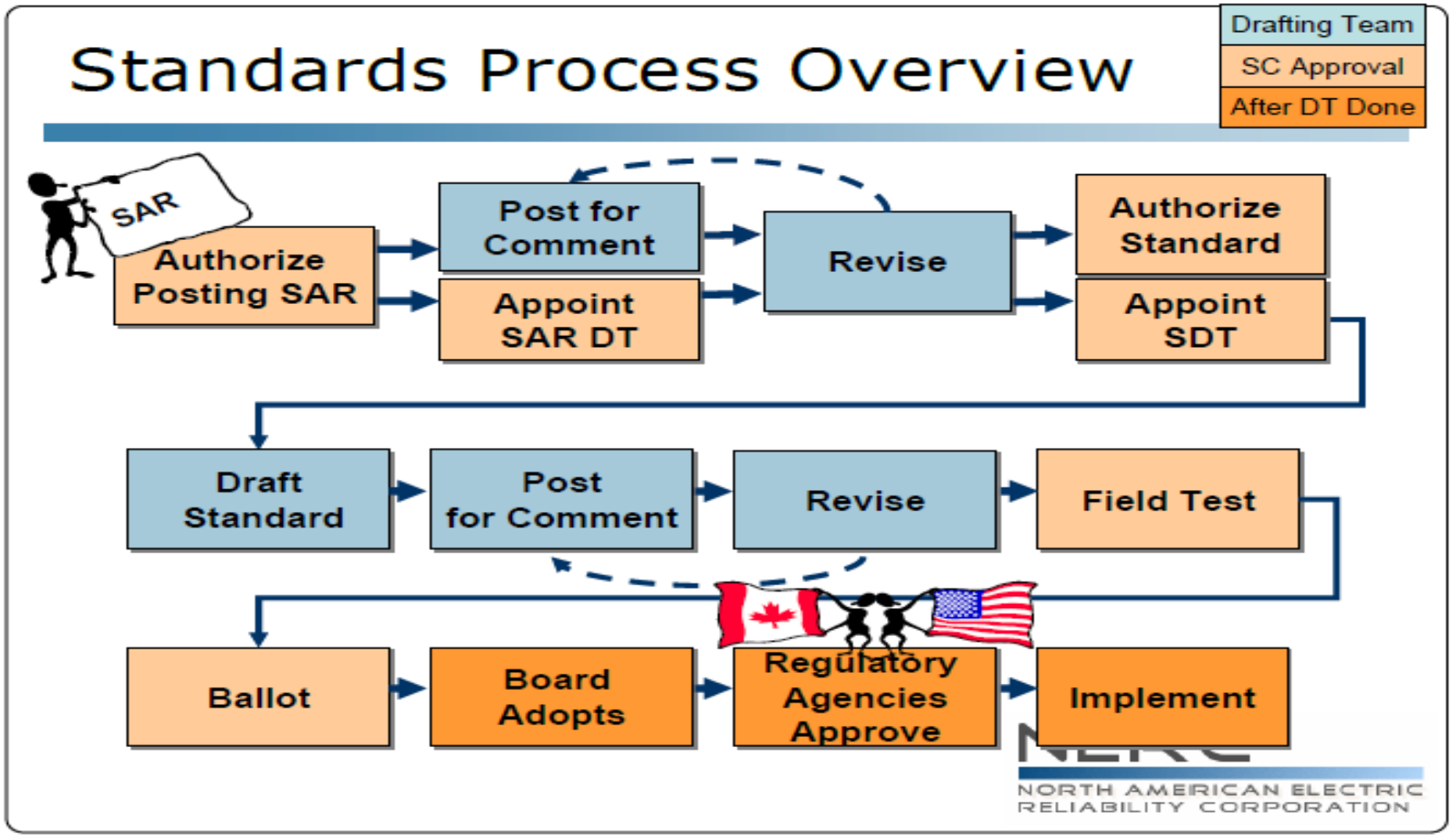
A quick history lesson

- 1965 Northeast Blackout
  - 30 million affected; one day
- North American Electric Reliability Council
  - Founded 1969
  - Creation of industry in U.S. and Canada
  - Voluntary standards for bulk power
- 2003 Northeast Blackout
  - 55 million affected; 2-7 days

How did we get here?

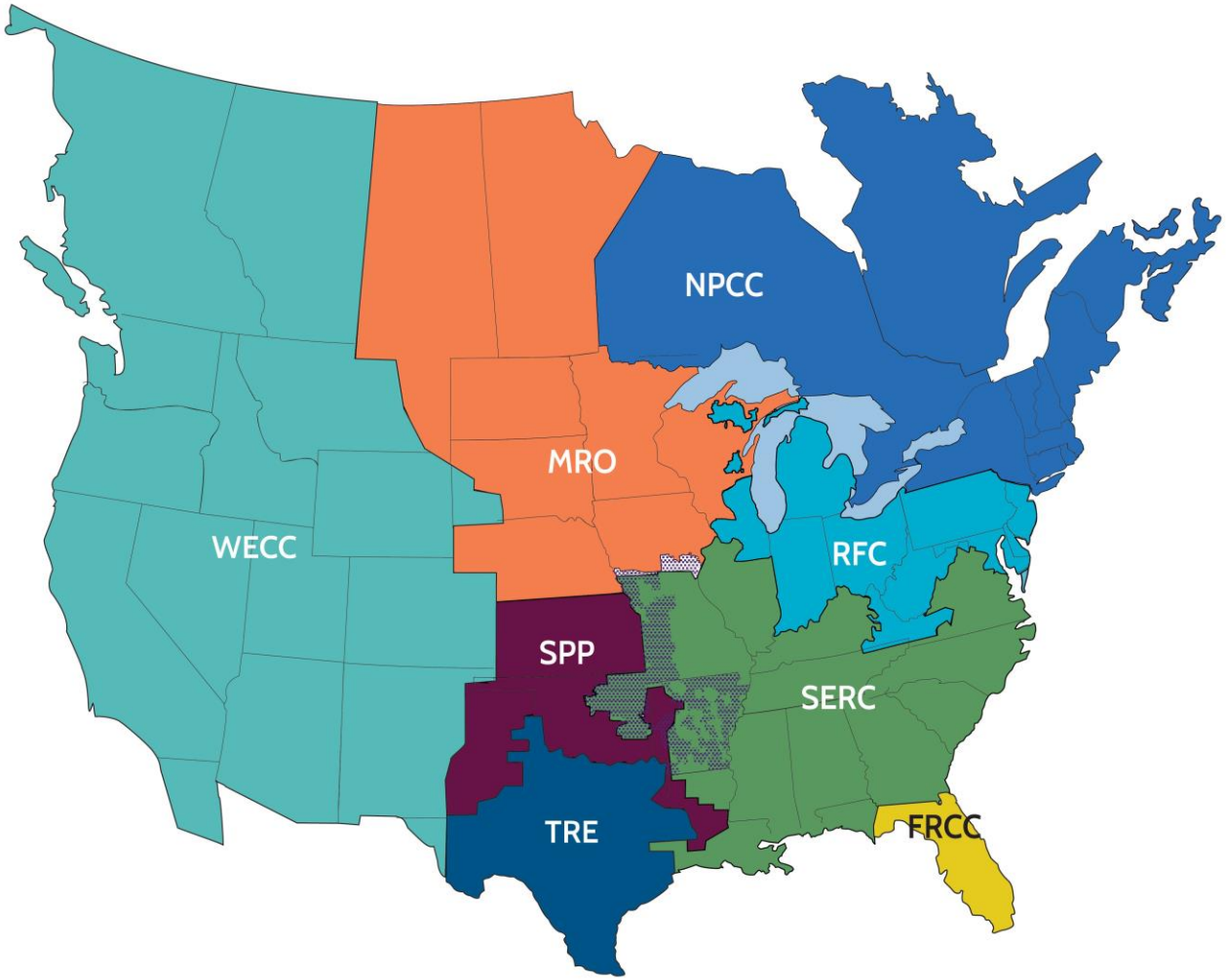
- Energy Policy Act of 2005
  - FERC to select an electric reliability organization -> NERC
- FERC Order No. 706 (January 2008)
  - Critical Infrastructure Protection (CIP) cyber security reliability standards
- NERC to draft and submit standards, for FERC's approval

How to make sausage



Who enforces all these rules?

- FERC
- NERC
- Regional Entities



Questions?

Thank you

We want your feedback! Use the conference app or visit the Registration desk.

Be sure to join the Twitter conversation: @CW_2016