

# Cybersecurity & Public Utility Commissions

**November 12, 2014**

**TCIPG**

Ann McCabe, Commissioner  
Illinois Commerce Commission

# NARUC

(National Association of Regulatory Utility Commissioners)

- **Cybersecurity Primer for State Regulators 2.0**, Feb 2013
- <http://www.naruc.org/Grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf>
  - Background
    - Prioritizing systems and networks over components
    - Ensuring that human factors are considered
    - Deploying defense-in-depth
    - Promoting system resilience
  - Sample questions for regulators to ask utilities
  - Workshops completed for 35 PUCs
- Special briefings, sharing best practices at NARUC meetings
- Resilience workshops & **Resilience in Regulated Utilities** paper Nov 2013, <http://www.naruc.org/News/default.cfm?pr=399>

# State PUC Issues, Challenges

- Oversee utilities' reliable operations and distribution
- Interest in third party audits, penetration testing
- Don't want information or plans that can't be protected (liability, confidentiality, FOIA)
- Emerging area: evaluating cyber-related expenses in rate cases
- "Internet of Things" is making the once air gapped ICS an easier target
- Often have limited technical knowledge, expertise
- Water/Energy nexus – one of many vulnerabilities
- Need public/private partnership that can meet current needs, flexible to meet evolving threats, bridge federal/state efforts

# State PUCs Overview

- Have adopted new rules and regulations
- Undergone education and training
- Had meetings and briefings with companies
- Opened dockets
- Consider cybersecurity in context of Advanced Metering Initiatives (AMI) - smart grid and smart meter
- Several states require cyber plans, e.g., AR, NY, PA
- Some require 3<sup>rd</sup> party audits, e.g., NY, TX
- Many dockets on access to customer data (e.g., AMI), both privacy and cybersecurity concerns

# State PUC Actions

- **WA** asks for voluntary CI Security Report, including physical and cyber, with specifics on electric utility's CI security team, training and occurrences
- **IN** held meetings with utilities, going on-site, hiring specialist
- **DC, IN** have been able to exempt certain info from FOIA
- **PA** goes on site to review practices, cyber plans; plans to do exercises on interoperability of CI
- **CA** has staff expertise, privacy initiatives and asks utilities how CI protected
- **TX** involved in response to threats

# State, Regional Efforts

- **FL** –small mgt audit group reviewing physical security of 4 IOUs and what they're doing vis-à-vis CIP 5 (report in Nov)
- **OH** met with major energy & water utilities and partner security agencies (state & federal)
- **CT** report to Governor urges third party audits
- **IL** requires submission of security plans
- **Middle Atlantic Cybersecurity Collaborative**
  - NJ, DC, PA, MD, DE, OH, NY
  - Goal: set forth best practices for state commission to effectively exercise their regulatory responsibilities over cyber security
  - asked NRRRI to gather state info, report soon

# State PUCs

- Cybersecurity considerations by PUCs thus far have been limited but continue to expand
- Approximately 15 commissions have adopted cybersecurity rules or opened cybersecurity dockets
- The focus on cybersecurity: system protection, reliability and/or resiliency

Understand that

- Cyber security is intrinsic to reliability
- Compliance does not mean security

# Questions for PUCs

- NARUC suggests questions in 5 areas: planning, standards, procurement practices, personnel and policies, and systems and operations
- Can your commission keep security information confidential?
- Do your reliability standards include cybersecurity considerations?
- Can you join incident response exercises by your utilities or Emergency Services Agency?
- Is there education that will enable staff to make prudency evaluations and recommendations re expenditures?
- Is there training/education available to enable staff to evaluate the effectiveness of utility cybersecurity plans?