The Evolving Role of State Regulation: A View from California

California Public Utilities Commission

Smart Grid Observer Cyber Security Virtual Summit

July 11, 2013

Opening Statements

- Cybersecurity should be considered a reliability effort
- State PUCs have jurisdiction over electric (and gas and water) utilities distribution networks, and oversee utility investment in that area
  - Utility rate cases, utility programs (EE, DR), retail market
- FERC maintains oversight over the “bulk power market,” i.e., the wholesale market and transmission network
  - North American Electric Reliability Corp (NERC) operating under the auspices of FERC defines and enforces reliability standards including cybersecurity requirements for the transmission network
- NERC’s Critical Infrastructure Protection (CIP) standards which relate to the preparedness and response to serious incidents is compliance based.
- On-going dialogue across the United States on moving to risk-based approach to cyber-security

Role of California PUC

- Regulate electric, natural gas, water, and telecommunications industries
  - Do not regulate municipal or cooperative utilities
- For electric industry, jurisdiction covers distribution grid and retail customers.
  - FERC has jurisdiction over wholesale markets and the transmission grid
- Every three years, or so, utilities filed General Rate Case (GRC) applications to cover expenses.
  - California is decoupled, so the PUC determines a Revenue Requirement for utilities (Phase 1) and then determines the rates to recover the Revenue Requirement (Phase 2)
- In GRCs, utility requests funding to cover operating costs
  - These requests include funding for cyber-security activities, etc.
- Responsible entity for ensuring utility operates in a safe, reliable, and secure manner at a reasonable cost.

Focus on Cybersecurity

- As utilities seek funding for new infrastructure investment, there should be a need by the PUC to ensure cybersecurity is accounted for in the request.

- Education and communication are key to effective regulation as well as reliable utilities.
  - On the regulation side, Commissioners, Administrative Law Judges, Advisors and Staff all need to understand the emergence of cybersecurity as a reliability factor.
  - On the utility front, IT departments need to build trust and understanding with field workers and electrical engineers.

- Cybersecurity practices are more effective when built into investments rather than bolted on later.

- Risk based approach to cybersecurity offers greater opportunity for utilities to address needs, risks, threats, and response
  - But there are regulatory challenges…..
  - And jurisdictional challenges…..

Jurisdictional Issues

- Transmission grid (over 100kV) and wholesale markets under FERC jurisdiction
  - NERC sets cybersecurity requirements
- Distribution grid and retail markets (under 100kV) under state/local jurisdiction
- Historically, distribution grid considered “dumber” than transmission grid, so less attention paid to cybersecurity.
  - However, with increased investment in advanced technologies on distribution grid, increased need to address cybersecurity
- Increased tension between Federal and local regulatory bodies as grid becomes more interconnected
  - Advanced meters
  - Distributed generation
  - Demand Response
- Efforts by Congress and Administration to mandate standards throughout electric grid

What Do PUCs Need to Know?

- Understanding a utility's process
  - What are the inputs?
  - Does the utility have an accurate inventory of its assets?
- Cyber threats and vulnerabilities evolve
  - A 3 year GRC cycle needs to allow sufficient flexibility to meet the changing threats
- Organizational integration
  - Is there sufficient buy-in across the business unit
- Use of standards
  - Voluntary vs mandatory
- Business case for cybersecurity (*i.e.*, cost)
  - How does one know the "right" amount of money to spend?
  - How does one know how effective the money was used?
  - Metrics

PUC Issues

- Limited staff available
- Expertise on technical aspects of cybersecurity needed
  - Who has time to participate in the myriad groups and activities?
- Valuing something that didn't happen
  - Complacency
  - Costs
- Regulatory construct related to pace of technological change
- What happens when a cyber-event happens?
- What is an acceptable level of risk?
- Where will Federal government jurisdiction come down?
- Coordination with other agencies, both state and Federal
- Pace of threats and vulnerabilities
- Access to classified materials and Federal briefings
  - PUCs likely have few to zero people with security clearances
- Reluctance to share information

Information Sharing

- Utilities (and vendors) need to be able to share information regarding threats and vulnerabilities
- Utilities should also be allowed to share info with regulatory body without fear of liability
- Safe Harbor rules may help with information sharing with regulatory bodies
- Regulatory bodies should be allowed to protect sensitive information from public release
  - Laws or rules may be needed to ensure data remains protected
- However, would like to have some information available publicly
  - Metrics

PUC White Paper Recommendations

- Suggests CPUC open a rulemaking to consider options for CPUC action on cybersecurity
- Cybersecurity framework should be based on a risk-based model
- Develop a means to evaluate utility investments in cybersecurity
- Develop a reporting protocol for cybersecurity incidents and information sharing regarding breaches and other incidents
- Develop an information sharing process that protects sensitive information from release
- Develop a Safe Harbor process to protect information sharing with the CPUC
- Develop a process for periodic reporting of security tests and audits

"The CPUC has a responsibility to ensure the safety and reliability of the grid down to the meter, and to ensure that utilities are prepared for the challenges of grid modernization as it occurs beyond their control. The CPUC also has a responsibility to ensure that ratepayer dollars are being invested effectively in cybersecurity." White Paper at 23.

Next Steps

- Exploration of cybersecurity framework for other industries, *i.e.*, natural gas and water.
  - To an extent, industries face same challenges: legacy vs advanced technology, IT vs ICS, need to protect infrastructure, need to provide for essential services
- Identification and adoption of metrics
  - Need for public reporting balanced with need to protect sensitive information
  - Should PUCs create/adopt standards
- Creating a culture of security
  - This is in addition to culture of safety
- Vendors
  - How to address supply chain risks
  - Shifting responsibility to vendors to meet cybersecurity requirements

Other States

- **Missouri Public Service Commission opened rulemaking (EW-2013-0011) in July 2012**
  - Asked 47 questions
  - Responses and reports filed under seal
- **Texas Public Utility Commission**
  - "Report on Electric Grid Cybersecurity in Texas," issued November 2012 (http://www.puc.texas.gov/industry/projects/electric/40128/PUCT_Project_40128_Electric_Grid_Cybersecurity_in_Texas.pdf)
- **Pennsylvania Public Utility Commission**
  - Utilities required to maintain cybersecurity continuity plans, and make available to PA PUC staff
  - PA PUC staff actively engages with utilities to review practices
- **Mid-Atlantic Commissions**
  - Joint regulatory effort to coordinate actions and outreach to utilities and other companies to develop a joint, regional plan for cybersecurity
  - Includes cooperatives, municipal and investor owned utilities, RTOs, FERC, natural gas, and water utilities.
  - Pennsylvania, Maryland, Delaware, D.C., and New Jersey commissions

For Further Information

CPUC Staff White Paper:
http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf

NARUC Cybersecurity for State Regulators:
http://www.naruc.org/Grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf

Marzia Zafar & Chris Villarreal
California Public Utilities Commission
Policy and Planning Division
Email: crv@cpuc.ca.gov and zaf@cpuc.ca.gov