

Commissioner Upendra J. Chivukula

I would like to thank Joe McClelland and FERC for providing me this opportunity to share my thoughts in this panel on “Incentives and Cost Recovery for Security Investments.” As we explore how federal and state authorities can provide incentives and cost recovery for security investments in energy infrastructure, I am very proud to state that NJ Board of Public Utilities (BPU) was the first state to issue a Cybersecurity Order in March 2016, specifying Cybersecurity Program requirements – Cyber Risk Management, Maintain Situational Analysis, Incident Reporting, Response and Recovery, and Security Awareness Training.

The cybersecurity journey began with NJ Legislature’s “Underground Facility Protection Act” in 2013 that required the utilities to submit data relevant to inquiry or investigation by board. Governor Christie established the New Jersey Cybersecurity and Communications Cell (NJCCIC) under the NJ Office of Homeland Security and Preparedness to coordinate cybersecurity information sharing and analysis among the government and private sectors.

A significant amount of utility infrastructure at risk falls within the purview of state public utility commissions (PUCs), who work to ensure safe, reliable, adequate utility service at reasonable rates. PUCs must make sure utilities are investing in security and ensure those investments are prudent. Security risk mitigation, can be accomplished using a variety of mitigation techniques, including administrative controls, such as, policies as well as technologies, for example, automated threat monitoring systems.

To execute their cybersecurity related responsibilities, PUCs must first know utilities’ business risk profiles, which include current and emerging physical and cyber security threats and vulnerabilities, and also have a working knowledge of best practice mitigation techniques. Information sharing, especially about threats and actual or potential incidents, is crucial for PUCs to be successful in this regard -- with federal partners including DHS, DOE, and FERC, with sector specific information sharing and analysis centers (ISACs), and with utilities themselves.

Armed with the cybersecurity knowledge, PUCs can assess utilities’ physical and cyber security preparedness and make prudency decisions:

1. Physical attacks: Physical attacks could render parts of the grid out of service for some period of time. Examples: Physical attack on the Metcalf substation; the as yet unrealized low probability/high consequence threat of an Electromagnetic Pulse (EMP) attack.
2. Cyberattacks - America’s intelligence community is raising alarms about cyber threats to critical infrastructure. The [Worldwide Threat Assessment](#) by Daniel R. Coats, the Director of National Intelligence contends that: China is able to launch cyber-attacks that cause localized, temporary disruptive effects on critical U.S. infrastructure – such as disruption of a natural gas pipeline for days to weeks and that Russia is able to execute cyber-attacks on electrical distribution networks —similar to those demonstrated in Ukraine in 2015 and 2016, and “is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.”

Utilities invest in technology to create business value - increased efficiency, which lowers overall costs. Digitalization of critical infrastructure supports reliability, efficiency, and cost effectiveness. Grid modernization embraces new operational technologies (OT) to achieve these benefits. New

technologies may also introduce unforeseen cyber vulnerabilities that put operational networks at risk of disruptions.

Cybersecurity investments are intended to protect the value that technology accrues. The rapid advancement of technology, increasingly interdependent infrastructures, and the growing threats to the energy infrastructure continue to challenge the level of protection that is required. Internet threat actors are intent on exploiting cyber vulnerabilities introduced by the operational complexity because of digitalization of networks.

PUCs must evaluate utilities' security preparedness in terms of risk to service reliability, safety and cost to customers. Some PUCs have enacted mandatory requirements and compliance thresholds (New Jersey, for example.) Others rely on informal means of gathering pertinent information from utilities, which include regular meetings to discuss their security risks and opportunities for risk reduction.

PUCs need to acquire a working knowledge of available alternatives and their efficacy to properly assess prudence, whether or not mandatory requirements exist. PUCs also need to understand the levels of investment, utilities are making for physical and cybersecurity. (Often, embedded in utilities' Information Technology budgets.)

PUCs need to conduct "mini" Black Sky Exercises to examine response and recovery roles and responsibilities and information sharing pathways.

PUCs need to be actively discussing cybersecurity resilience – what it is, how to measure it, and how to incentivize it examining "resilience risks" associated with infrastructure interdependencies.

Cost recovery also is a means to incentivize security preparedness. The range of cost recovery mechanisms for security investments is well known. The most familiar is filing a general rate case. Currently, FERC and different states typically require utilities to propose recovery for needed cybersecurity investments as part of broader comprehensive rate change requests. rather than allowing them to make those proposals separately. A 2017 survey by the National Renewable Energy Laboratory (NREL) suggests among those surveyed, that base rate "is the most popular mechanism for recovering cybersecurity expenses: it was selected by 10 of the 22 utilities, and 8 of the 19 non-NERC utilities."

PUCs are working with National Association of Regulatory Utility Commissions (NARUC) that is working to advance PUCs' knowledge of physical and cybersecurity risks, enhance awareness of best practice risk management practices, and provides tools to assess utilities' implementation of those practices; PUC Commissioners need to participate in "Cybersecurity Training for Regulators" to obtain working knowledge needed for utility oversight.

The 2018 NARUC survey with 21 PUCs responding, found about half of those responding have legislation, rules, or administrative orders requiring utilities to provide information on cyber practices, threats and incidents to the PUC. A third require auditing, evaluations, or assessments of utilities' cyber capabilities. Capabilities are most often assessed against NERC CIP and NIST Cybersecurity Framework.

A recent unpublished survey of 22 PUCs by NRRI supports NREL's findings that most cyber costs show up as part of IT budgets. Although cost recovery is mainly through rate cases, some states allow recovery outside of rate cases through security or infrastructure riders.