PURC Working Paper

State Public Utility Commissions' Role in Cybersecurity and Physical Security Issues: Trade-Offs and Challenges

Lynne Holt, Policy Analyst, and Mary Galligan, PURC Senior Fellow

December 12, 2017

A. Introduction

The US electric power grid, broadly defined, has long been recognized as a viable target for cyber threats. The grid has been described as "a highly complex enterprise: 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines; 55,000 substations; and 5.5 million miles of distribution lines that bring power to millions of homes and businesses."[1] In the usual course of business, if something goes wrong, either due to human error or ill intent, a generally predetermined set of actions is executed to respond to the problem. Electric utilities have a lengthy experience in responding to weather-related events such as ice storms, floods, and hurricanes. Historically, utilities have had less experience with human threats and attacks, especially those aimed at digital systems that are increasingly important to efficient operation. A recent MIT whitepaper on cybersecurity noted:

> Cyber threats and cyber-attacks can come from a variety of malicious actors, such as foreign nations, terrorist organizations, private firms, external hackers, or internal "bad actors" among system operators, power companies, and vendors. These actors may seek to disrupt grid operations, damage infrastructure, or steal information. They may hire criminal organizations to attack utility grids to disrupt network controls and generation for political reasons, or for economic gain using "ransomware."[2]

The potential for cyberattacks is a growing concern for electric utilities. In a 2017 survey of 600 electric utility executives conducted by Utility Dive, 72% of respondents indicated that physical and cyber threats were important or very important concerns and priorities.[3] That response represented an elevated concern with such threats in 2017, compared to responses provided in 2015 and 2016.[4]

Cybersecurity concerns are based in reality. According to the federal Department of Energy's (DOE) "Quadrennial Energy Review," "Cyber threats to the electricity system are increasing in sophistication,

---

[1] Robert K. Knake, *A Cyberattack on the U.S. Power Grid*, Council on Foreign Relations, April 2017, 1, https://www.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf. Last accessed December 4, 2017.

[2] Cyril W. Draffin, Jr., *Cybersecurity White Paper,* MIT Energy Initiative Utility of the Future, December 15, 2016, https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf. Last accessed December 4, 2017.

[3] Herman K. Trabish, "Why Utilities Say Grid Security is the Most Pressing Sector Issue of 2017," *Utility Dive*, April 10, 2017, https://www.utilitydive.com/news/why-utilities-say-grid-security-is-the-most-pressing-sector-issue-of-2017/440056/. Last accessed December 4, 2017.

[4] Ibid.

magnitude, and frequency."[5] Recent reports suggest that cyber threats to US energy companies have moved to a new level. In the spring and summer of 2017, targeted companies' networks were hacked and at several US energy companies the attackers gained "operational access: control of the interfaces power companies use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses."[6]

In the early summer of 2017 there were reports of cyberattacks on "multiple nuclear power generation sites" in the US.[7] Just prior to those reported incidents, the North American Electric Reliability Corporation (NERC)[8] issued a public alert about the malware that knocked out power in Ukraine and a warning about North Korean threats to US critical infrastructure.[9] The nuclear facility in Kansas was one of the facilities hacked in early 2017. Public reports did not indicate that control systems were breached, but the joint report issued by the Department of Homeland Security (DHS) and the FBI classified the threat as "urgent amber," the second-highest category of threat sensitivity. Separation of business and operational networks at nuclear plants may be more extensive than at other plants, thereby providing a level of protection.[10]

The US power grid is not the only one being threatened. In 2015 nearly 250,000 Ukrainians lost their electrical service due to a cyberattack and approximately a year later a transmission station in Ukraine was taken off line by another cyberattack. Both Ukrainian attacks were linked to Russia and six months after the most recent attack, experts speculated that the malware used against Ukraine could be used nearly anywhere in the world.[11] Scottish Power in the United Kingdom and Iberdrola and Gas Natural in Spain were all impacted during the spring of 2017 by a ransomware worm that infected computer systems in nearly 100 countries.

While cybersecurity is needed at all levels of the grid, PUCs share oversight and responsibility for developing security standards for electric utilities with the Federal Energy Regulatory Commission (FERC), the DOE, NERC and the National Institute of Standards and Technology (NIST) but the state role when it comes to

---

[5] US Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the QER*, January 2017, 7-22, https://energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf, Last accessed December 4, 2017.

[6] Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," *Wired*, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/. Last accessed December 4, 2017. See also Ellen Nakashima, "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks," *The Washington Post*, July 8, 2017, https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.2e7019306d3e. Last accessed December 4, 2017.

[7] Blake Sobczak and Peter Behr., "Nuclear Breach Opens New Chapter in Cyber Struggle." *E&E News.* June 27, 2017,https://www.eenews.net/stories/1060056628. Last accessed December 4, 2017.

[8] NERC is a not-for profit organization whose members are users, owners, and operators of bulk power which is authorized to propose and update reliability standards for critical infrastructure protection.

[9] Sobczak and Behr, ftn. 7.

[10] Nicole Perlroth, "Hackers are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I Say," *The New York Times,* July 6, 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0&_r=0.. Last accessed December 4, 2017.

[11] Jim Finkle, "Cyber Firms Warn of Malware That Could Cause Power Outages." Reuters.com. June 12, 2017, https://www.reuters.com/article/us-cyber-attack-utilities/cyber-firms-warn-of-malware-that-could-cause-power-outages-idUSKBN1931EG. Last accessed December 4, 2017.

cybersecurity is often less defined. The MIT whitepaper noted: "Some state public utility commissions have started to address cybersecurity challenges at the distribution level, but more decisive actions are required."[12] The need for more state-level action was underscored by a simulated attack orchestrated by NERC's GridEX III which convened 4,400 people from 364 organizations in North America, including utilities, law enforcement, and other government agencies. In March 2016 NERC released a report about the exercise, finding that cybersecurity improvements were needed in the distribution system, including information sharing and communication, simplifying electric system operations to provide basic services, and establishing priorities for electricity service restoration.[13]

Even prior to that NERC assessment, state regulators acted through the National Association of Regulatory Utility Commissioners (NARUC), to tackle security and reliability issues potentially affecting their oversight of the grid. NARUC established the Critical Infrastructure Resource Center whose mission is to "provide a central location for Commissioners and staff to go to find relevant, timely information on critical infrastructure reliability, security and resilience topics: physical security, cyber security, and operational security."[14] The Center published its initial primer, *Cybersecurity: A Primer for State Utility Regulators,* in 2012 and updated it most recently in January 2017.[15] The primer provides an overview of cybersecurity issues, challenges, practices, and standards governing utilities to make their systems less vulnerable to potential threats. The primer also identifies key concepts for regulators' considerations in their assessments of utility cybersecurity proposals. These concepts include the following: "prioritizing systems and networks over components; ensuring that human factors are considered; deploying defense-in-depth; promoting system resilience."[16]

This paper concerns itself with the role of the state public utility commissions (PUC) in contributing to improved cybersecurity practices on the part of jurisdictional electric utilities as they plan and position themselves for potential cyber threats and attacks. PUCs make decisions regarding the nature and extent of their involvement in protecting distribution operations and facilities from external and internal threats. If they decide to require utilities to undertake enhanced cybersecurity measures, what challenges and trade-offs are PUCs likely to encounter?

This paper addresses those questions by exploring briefly:

- several areas of concern facing PUCs as they seek to encourage electric utilities to become more resilient in protecting themselves and their customers from cyber threats
- Connecticut as an example of one means of overseeing utility risk management/mitigation efforts

---

[12] Draffin, ftn. 2.

[13] NERC, *Grid Security Exercise: GridEx III Report*, March 2016, http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf. Last accessed December 4, 2017.

[14] National Association of Regulatory Utility Commissions (NARUC) "Committee on Critical Infrastructure," NARUC Summer Policy Summit, https://pubs.naruc.org/pub.cfm?id=954BD7F9-F3E3-08A0-E2CB-740696755E50. Last accessed December 4, 2017.

[15] Miles Keogh and Sharon Thomas, Cybersecurity: *A Primer for State Utility Regulators,* Version 3, NARUC, January 2017, https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F. Last accessed December 4, 2017. The primer may go toward meeting Overarching Recommendation 7B contained of the consensus study report of the National Academies of Sciences, Engineering and Medicine, *Enhancing the Resilience of the Nation's Electricity System*, National Academies Press: Washington, D.C. 2017, p. 7-6.

[16] Ibid., at 13.

- policy questions and trade-offs that PUCs will need to confront as they determine how best to contribute to reducing vulnerabilities of customers and utilities in their respective jurisdictions.

B. Challenges Facing State Public Utility Commissions

The smart grid[17] has been identified as a source of vulnerability in the electric network at the distribution system level. Although the smart grid has not been widely implemented to date, security concerns are raised by utilities, regulators, and customers. Thus, incorporation of smart grid technologies into the distribution network and the recognition that those technologies make the grid increasingly vulnerable have created policy questions for PUCs with respect to: 1. protection of sensitive customer-related data and information; 2. confidentiality of data used in security planning, implementation and risk mitigation; 3. cost-recovery for utility investments in cybersecurity-related improvements; 4. skills needed in the utility workforce to improve its resilience to external threats; and 5. approaches taken by utilities to reduce vulnerabilities on the grid.

1. Customer Data Privacy Protection:

Privacy protection is a pressing concern as the electric grid becomes more reliant on distributed energy resources (DERs) and the number of electric and telecommunications devices proliferates on the grid. As the MIT whitepaper put it:

> If electric utilities begin to collaborate more with device control system aggregators, electric car owners, and vehicle charging aggregators, specific procedures to protect [against] data breaches and information exfiltration will be required. The challenge is to simultaneously protect legitimate customer expectations of privacy, be a good steward of data, and apply analytics to create additional value for consumers.[18]

At the heart of this collaboration are technologies that enable two-way communications with the electric system, providing numerous, and often unprotected, entry points to the grid. Attackers can exploit vulnerabilities exposed by these entry points to gather private information being used and transmitted by smart grid devices, inflict local damage, or cause more extensive damage to the network.

Two types of attacks pose specific threats to privacy: 1. attacks that attempt to capture consumption data in transit, and 2. attacks on stored data. Either cache of data may include more than just energy consumption information and could constitute an invasion of a customer's privacy. For example, real-time surveillance could capture data in transit, revealing whether an individual is present in a home or a resident's behavior pattern. Likewise, a real-time data capture could reveal when a business is engaged in production or other processes. Larger caches of customer data transmitted via the smart grid to a utility or related service provider and stored for legitimate purposes related to the services provided could be accessed, if

[17] The term "smart grid" is defined as "Modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a 'dialogue' between all components of the grid, and allowing for automatic command and response within the function of the grid." See Keogh and Thomas, ftn. 15, Appendix B.
[18] Draffin, ftn. 2, at 15.

not sufficiently secured, by unauthorized entities such as marketers or governmental entities who would have an interest in other information about customers' longer-term patterns of activity. Once captured, consumption data can be disaggregated into individual electricity use patterns (load signatures) and analyzed for forecasts about household or business activities.[19, 20]

If PUCs are interested in supporting continued modernization of the grid by incorporating smart grid technology, maintaining customer confidence related to private data will be key. State laws may need to be examined to ensure that PUCs have requisite authority to prevent inappropriate or illegal customer data disclosure. At the federal level, President Obama initiated an effort to address customer data privacy through the formation of the Smart Grid Interoperability Panel Cyber Security Working Group which issued guidelines for smart grid cybersecurity in September 2010,[21] revised in September 2014.[22] The Obama administration issued in January 2015 concepts and principles for a voluntary code of conduct for utilities and third parties governing the privacy of data related to customer energy usage. Those concepts and principles were the product of a 22-month multi-stakeholder effort that was facilitated by the Office of Electricity Delivery and Energy Reliability, DOE, in coordination with the Federal Smart Grid Task Force.[23]

For their part, states have acted upon the treatment of privacy of customer data. As of April 2017, 48 states and the District of Columbia had security breach laws. The only states lacking such laws were South Dakota and Alabama.[24] PUC involvement stepped up as smart grid technology adoption was stimulated by the availability of federal moneys through the American Recovery and Reinvestment Act of 2009. In 2011, for example, the PUCs in California, New York, Colorado, and Ohio initiated regulatory proceedings dealing with customer privacy and security protections. Other PUCs followed suit and several, including Connecticut discussed below, adopted policies regarding third-party access to customer data, either through legislation or PUC regulation. Among those states with privacy protection policies, customer consent is typically

---

[19] Nico Saputro and Kemal Akkaya, "On Preserving User Privacy in Smart Grid Advanced Metering Infrastructure Applications," S*ecurity and Communication Networks,* 7 (1), January 2014, 206-220.

[20] Telecommunication services that interface with smart grid devices may be equally problematic from the perspective of possible disclosure of personal information. Blurring functional lines of types of utilities poses its own set of challenges for regulators that are beyond the scope of this paper.

[21] NIST, I*ntroduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security: The Smart Grid Interoperability Panel*, Cyber Security Working Group, September 2010, https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf. Last accessed December 4, 2017.

[22] NIST, *NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, September 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. Last accessed December 4, 2017. Among the additions to the initial framework was the inclusion of a risk management framework for the electricity subsector to provide guidance on security practices.

[23] See Smartgrid.gov, *Dataguard Energy Data Privacy Program*, https://www.smartgrid.gov/data_guard.html. Last accessed December 4, 2017. The Federal Smart Grid Task Force was established under Title XIII of the Energy Independence and Security Act of 2007.

[24] Iauen Jolly, "Data Protection in the United States: Overview," Law stated as at 01 Jul 2017, Thomas Reuters Practical Law, https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1. Last accessed December 4, 2017.

required as a precondition for sharing customer data.[25] As one report that summarized these state regulatory actions observed:

> While there is no doubt that the deployment of smart grid technology will be key to the creation of a more energy efficient economy, maintaining privacy rights over the data created is going to be critical to the public's acceptance of such technology and the success of the smart grid as a whole. It will be up to governments and utilities [sic] regulators over the next couple of years to enact sound policies that ensure the privacy and security of customer information without placing undue and restrictive burdens on smart grid and utility companies.[26]

2. Confidentiality of information related to utility security

Securing the US power grid against a physical or cyberattack is a daunting task for regulators because 90% of the grid is privately owned, highly decentralized and US power plants are aging. According to April 2016 testimony to Congress by the Congressional Research Service, "As of 2009, the average age of power plants was over 30 years, with most of these facilities having a life expectancy of 40 years. Electric transmission and distribution system components are similarly aging, with power transformers averaging over 40 years of age, and 70% of transmission lines being 25 years old or older, as of 2007."[27]

PUCs need to be able to access information about proposed cybersecurity improvements for cost-recovery proceedings. These investments might take the form of employee salaries and technology needed to comply with federal regulations and related standards. Determining the prudency of a security-related investments can be very complicated. This is especially the case when upgrades that appear to be unrelated to security, introduce vulnerabilities, or otherwise increase risks, e.g., switching from manual to automated operating processes.

Protection of confidential information provided by utilities, as authorized by state statutes, can make the difference as to whether utilities will be more or less inclined to share security-related information with the PUC and its staff. As a National Regulatory Research Institute report on cybersecurity stated:

> As government institutions, many state utility commissions must disclose their actions and open their hearings to the public. Unless properly shielded via clearly defined statutory protections, Freedom of Information requests can expose information provided to a state agency about a utility's cybersecurity plans. Due to this concern, utilities may be hesitant to provide cybersecurity

[25] American Council for an Energy Efficient Economy, State and Local Policy Database, "Data Access.," https://database.aceee.org/state/data-access. Last accessed December 5, 2017.
[26] Julia M. Siripurapu, Cynthia J. Larose, Billy Najam, and Devon Cain, "Privacy and the Smart Grid: Utilities Regulators and the Adoption of Smart Grid Data Protection Rules," MintzLevin, September 20, 2011, https://www.mintz.com/newsletter/2011/Advisories/1377-0911-NA-cECT/web.htm. Last accessed December 4, 2017.
[27] Testimony by Richard Campbell, as cited in Kevin Begos, "Protecting the Power Grid," *CQ Researcher*, 40(26), November 11, 2016, http://library.cqpress.com/cqresearcher/getpdf.php?id=cqresrre2016111100. Last Accessed December 5, 2017.

information to commissions. This, in turn, makes it difficult for commissions to assess the prudence of a utility's request to recover costs for expenses related to cybersecurity.[28]

Some states have more liberal open records laws than do others. For example, Illinois' Freedom of information Act appears to provide fewer protections to utilities than does the Indiana law which provides numerous protections.[29] Florida has among the strongest "sunshine" laws in the nation. Therefore, utilities in the state may be reluctant to share cyber-related information with the Florida Public Service Commission even though there are exemptions from public records disclosure in Florida's statutes for "proprietary confidential business information" which includes, among others, "security measures, systems, or procedures." To trigger the exemption, the Florida Public Service Commission must first determine whether the information affects a utility's rates or cost of service. The Commission may issue an order to protect the information from public disclosure upon a finding that disclosure is in the public interest. The duration of the protective order would not generally exceed 18 months.[30]

Municipal utilities may not necessarily be protected from open public records laws if the PUC has no ratemaking jurisdiction over them. Such was the case in Florida until recently. The 2016 Florida Legislature enacted legislation to exempt Florida's municipal utilities' security measures, including security of information technology systems, from the state's open records act.[31]

Many states have statutes that exempt utility cyber-security plans and related information from public scrutiny. The National Conference of State Legislatures (NCSL) conducted a survey in February 2017 posing questions related to cybersecurity practices. Of 22 commissions that responded, 19 indicated that they are authorized to protect certain data from public disclosure.[32] Despite these laws, utilities might be uneasy to share some types of sensitive information with their regulators. In response to the survey, only nine commissions replied that someone at the PUC had formal security clearance and 13 responded that the necessary rules existed regarding the recipients of such information. The issue of formal security clearances becomes particularly important for developing the cross-jurisdictional relationships necessary for robust cybersecurity.

---

[28] Daniel Phelan, "*Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues ,"*National Regulatory Research Institute, Report Bo. 14-12, December 2014, 6-7, http://www.energycollection.us/Companies/NRRI/Summary-State-Regulators.pdf. Last accessed December 5, 2017.

[29] Commissioner Sherina Maye Edwards and Caitlin Shields, with Anne McKeon and Nakhia Crossley, "Cybersecurity: Part 1," *Public Utilities Fortnightly,* February 2017, https://www.fortnightly.com/fortnightly/2017/02/cybersecurity-part-1?authkey=c4869ac2fb271e063b0930630283c52c7aba2cfba161060eadfcc5121603ca5f. Last accessed December 5, 2017.

[30] F.S. 366.093.

[31] Ch. 2016-95, L.O.F. For a summary of the legislation, see http://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=h1025z1.EUS.DOCX&DocumentType=Analysis&BillNumber=1025&Session=2016.

[32] Richard Mroz, "CI Survey Response Summary," Critical Infrastructure Committee, NCSL, February 12, 2017. See also, National Conference of State Legislatures, "Cybersecurity Legislation 2017," October 30, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx#2017 [noting that among the cybersecurity topics considered by state legislatures in 2017 were bills restricting disclosure of sensitive security information.] Last accessed December 5, 2017.

PUCs' ability to share cybersecurity information with other parties is a related issue. As described here and elsewhere in the utility-related cybersecurity literature, a number of state, federal, and local entities are charged with various aspects of ensuring the security of the electric grid and other elements of the utility network. The concept of partnership in this area of electric system operation and regulation is not out of step with joint jurisdiction over utilities in many other areas. However, there are unique considerations in the area of cybersecurity that present challenges for each jurisdictional level. The nature of the electricity generation and distribution systems mitigates against a piecemeal approach to securing the grid. A vulnerability at the distribution level can quickly have adverse impacts on distant utilities crossing jurisdictional lines that serve the industry well in other contexts. Information must be shared in a secure and responsible manner among relevant regulators, enforcement, and recovery entities.

Recent recommendations by the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative included a number of steps, largely led by industry and supported by the public sector that could create an approach to implementing cybersecurity. Among the findings of the report is that the electric industry may not be able to obtain "timely, specific, and actionable" intelligence information from government agencies.[33] Policy recommendations to encourage information sharing include two of particular interest in regard to cross-jurisdictional issues:

- The US intelligence community, DHS, and DOE should conduct regular outreach to state utility commissioners, other relevant state agencies, and public and municipal utilities on cyber threats and vulnerabilities. These federal agencies should identify best practices for sharing classified information with private sector entities as needed to protect critical infrastructure.
- US intelligence officials should conduct regular outreach and briefings, including classified briefings with relevant state officials and with Canadian and Mexican industry counterparts. DHS and DOE should also work to ensure that these counterparts are able to engage in all relevant government-industry forums.[34]

Partnerships may extend into the cyber realm as well. High performing computing and artificial intelligence may be useful tools with which to identify and develop protections against cyber threats.[35]

Finally, PUC cybersecurity partnerships often operate in the larger sphere of state government. Many governors have taken the initiative to incorporate cybersecurity considerations into their energy assurance plans. Elements of those plans include assigning specific roles and responsibilities to agencies across state government, promoting best practices and risk-based security assessments among utilities, convening the

[33] Michael Hayden, Curt Hebert, Susan Tierny, co-chairs, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*, A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative, February 2014, 11 https://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf. Last accessed December 5, 2017.
[34] Ibid., p.12
[35] Deborah Evanson, "Internet of things" Makes Us Vulnerable to Cyber-attack - Imperial Expert," Imperial College London. February 28, 2017, http://www3.imperial.ac.uk/newsandeventspggrp/imperialcollege/newssummary/news_28-2-2017-14-5-26. Last accessed December 5, 2017.

many state and regional entities involved in cybersecurity, and encouraging creation of cybersecurity expertise in traditional emergency response entities such as the National Guard.[36]

3. Cost-recovery for utility investments in cybersecurity investments

Assuming a PUC can access the requisite data with which to determine whether cybersecurity investments were prudent, the commission will need expertise in making such an evaluation. That task becomes increasingly challenging as the electric utility's information technology (IT) systems connect increasingly with its operational-technology (OT) networks. The OT system supports generation and distribution power over large areas.[37] In the past, OT systems operated in relative isolation and had proprietary protocols that were difficult for mal-intentioned parties to penetrate. As OT systems gained capabilities for data generation, billing, customer service, forecasting and other responsibilities, there was more of a push to connect the OT systems with IT systems. To enable that connectivity, the proprietary protocols of OT systems have been gradually replaced by more standardized hardware and operating systems. The standardized systems are more familiar to attackers. The connectivity of IT and OT systems may be out of sync since the replacement cycle of OT technology tends to be of a much longer duration than that of IT-based industries.[38]

Many utilities have system and network architecture that predates current cybersecurity concerns and have added layers to the legacy systems. Sometimes those added layers include security measures. Among the many challenges electric utilities face, legacy technologies may be the most pressing, particularly for utilities that are required to comply with Critical Infrastructure Protection (CIP) standards.[39] These standards are approved by the FERC, which regulates bulk power in interstate commerce. NERC's CIP standards currently do not apply to local distribution utilities. Consistent with NERC's mission focusing on reliability, cyber

[36] Andrew Kambour, "Enhancing the Cybersecurity of Energy Systems and Infrastructure," NGA Paper, National Governors Association Center for Best Practices, August 4, 2014, https://www.nga.org/files/live/sites/NGA/files/pdf/2014/1408EnhancingCybersecurityEnergySystems.pdf. Last accessed December 5, 2017.

[37] The following is an explanation of Operations Technology (OT): "OT encompasses operating gear, from oil circuit breakers and sectionalizers to solid-state relays, and many devices in between. OT also often includes control room applications, such as supervisory control and data acquisition (SCADA) systems that monitor the network, reaching out to devices as complex as substation gateways, or as simple as sensors. OT is often applied within a mission-critical framework and is recognizable to every person working in utility operations, but it is seldom, if ever, considered or understood by anyone else." See Jeff Meyers, P.E., *How the Convergence of IT and OT Enables Smart Grid Development*, Schneider Electric White Paper, 2013, 2, http://cdn.iotwf.com/resources/10/How-the-Convergence-of-IT-and-OT-Enables-Smart-Grid-Development_2013.pdf. Last accessed December 5, 2017.

[38] Nadya Bartol, Michael Coden, David Gee, and Craig Lawton, *Ensuring Cybersecurity in the Electric Utility Industry*, BCG, August 16, 2017, https://www.bcg.com/publications/2017/power-utilities-technology-digital-ensuring-cybersecurity-electric-utility-industry.aspx. Last accessed December 5, 2017.

[39] The National Renewable Energy Laboratory (NREL) asked 22 electric utilities (19 of which were not required to comply with CIP standards) about challenges they faced in cybersecurity and they were given nine possible responses. Legacy technology was cited by more electric utilities that were not NERC-compliant than was any other challenge. See Ivonne Pena, Michael Ingram, and Maurice Martin, *States of Cybersecurity: Electricity Distribution System Discussions*, NREL, Technical Report NREL/TP-5C00-67198, March 2017, https://www.nrel.gov/docs/fy17osti/67198.pdf. Last accessed December 5, 2017.

threats that fall short of disrupting service, such as breaching customer privacy or disrupting business processes, may not be addressed by those standards.

FERC Order No. 829, issued in July 2016, asked NERC to develop standards to improve the reliability of the supply chain for the bulk electric system (BES), reflecting the evolving architecture and connectivity between IT and OT systems referenced above. FERC's order asked NERC to address four areas: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls.[40] In its order, FERC observed: "The targeting of vendors and software applications with potentially broad access to BES Cyber Systems marks a turning point in that it is no longer sufficient to focus protection strategies exclusively on post-acquisition activities at individual entities."[41] Although most of the standards apply to entities covered under BES, there is a limited application to distribution providers that own facilities, systems, and equipment for the protection or restoration of the BES.[42]

Given the evolving nature of the technology, one might ask how PUCs evaluate security measures, including cybersecurity. A Missouri commissioner observed that well-established precedents do not exist for regulators to evaluate them and typically, the PUC must rely on the testimony of witnesses in proceedings to make such determinations.[43] PUCs must guard against underinvestment, on the one hand, and excessive or inappropriate investment on the other hand. One means of informing evaluations is to ensure that utilities have an effective security plan which addresses vulnerabilities, threats, mitigation, chain of command for emergency response, communications to the public, continuity of operations, damage assessment, response and recovery, and interactions with other government emergency response personnel.[44]

4. Workforce skills needed by the utility to improve its resilience

While one might not expect PUCs to have a direct role in training utility personnel for cybersecurity compliance, they must be cognizant of the challenges facing utilities in securing the appropriate workforce. Any assessment of the prudency of security investments must include the utility's ability to implement the security measures. Thus, the availability of appropriately skilled workers should factor into the analysis.

---

[40] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 FERC ¶ 61,050 (2016).

[41] Ibid., 33.

[42] These facilities, systems, and equipment are specified in Applicability Section 4.1.2 of the NERC proposed standards. See NERC, Docket No. _____*Petition of the North American Electric Reliability Corporation for Approval of Proposed reliability Standards CIP-013-1, CIP-005-6, AND CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, September 26, 2017, http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20Supply%20Chain%20Risk%20Management%20Filing.pdf. Last accessed December 5, 2017.

[43] Terry M. Jarrett, Commissioner, Missouri Public Service Commission, "Protecting Utilities' Critical Infrastructure: the PSC's Role," no date, https://psc.mo.gov/CMSInternetData/Commissioners/TerryMJarrett/Protecting%20Utilities%20Critical%20Infrastructure.pdf. Last accessed December 5, 2017.

[44] Ibid.

NERC identified human performance as one of the major risk factors to reliability in its *Compliance Monitoring and Enforcement Implementation Plan* because the most critical risk factor is decision-making in both real time and in system planning.[45] One might ask whether the electric power industry has the workforce it needs to comply with NERC's standards. Estimates at the international level are not encouraging, with one analysis projecting a global shortfall of 1.8 million cybersecurity professionals by 2022. Moreover, fewer than 25% of applicants are expected to be qualified.[46]

The presence of more networked systems, including elements of the smart grid, mean qualifications for positions in the electric power sector are changing drastically. Specifically, there is a greater need for the power grid workforce to understand, design, and manage what are known as cyber-physical systems (CPS).[47] In addition, the workforce will need proficiency in risk management, behavioral science, and identifying cybersecurity risk factors.[48] Even if the hardware and operating systems are converging for OT and IT, the applications and goals are not. Utilities also will need employees who are familiar with both IT and OT applications in the new environment of OT and IT connectivity. This will likely be a challenge.[49]

Finally, utilities will need a cadre of employees possessing a new set of skills, i.e., security professionals with backgrounds and expertise in intelligence, the military, and law enforcement who can take information concerning cyber threats received and validated by federal intelligence agencies and translate that information into actions.[50] Professionals with these skills are generally more expensive to hire and retain than those with traditional security skills found among existing utility staff.

5. Approaches by utilities to reduce vulnerabilities on the grid

There are two general, but complementary, approaches utilities can undertake in implementing cybersecurity measures. One approach is compliance with CIP standards developed by NERC and approved by FERC.[51] Beyond simple compliance, utilities can take a risk-based approach which involves setting priorities based on the value assigned to the data or system that could be compromised through access by

[45] NERC, 2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan Version 2.4, March 2017, http://www.nerc.com/pa/comp/Resources/ResourcesDL/2017_ERO_CMEP_IP.pdf.

[46] The BCG analysis (Bartol *et al*., ftn. 39) is based on ISC Blog, "2017 Global Information Security Workforce Study," *ISACA 2017 State of Cybersecurity*, 4.

[47] CPS is defined as "cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. In cyber-physical systems, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context." See Wikipedia, https://en.wikipedia.org/wiki/Cyber-physical_system. Last accessed December 5, 2017.

[48] *Transforming the Nation's Electricity Sector*, ftn. 5, at 5-10.

[49] Bartol *et al*., ftn. 38.

[50] Brian Harrell, "Public-Private Cyber Threat Intelligence Sharing Necessary in Electricity Industry," *CSO online*, February 12. 2016. https://www.csoonline.com/article/3032347/security/public-private-cyber-threat-intelligence-sharing-necessary-in-electricity-industry.html. Last accessed December 5, 2017.

[51] Utilities received some feedback from FERC on successes and deficiencies with CIP compliance efforts through FERC staff audits conducted in FY 2016 and FY 2017, respectively. See FERC, *2017 Staff Report: Lessons Learned from Commission-Led CIP Version 5 Reliability Audits*, October 2017, https://www.ferc.gov/legal/staff-reports/2017/10-06-17-CIP-audits-report.pdf Last accessed December 5, 2017.

a malicious actor.[52] The cybersecurity framework developed by the NIST[53] embodies a risk-based approach as does the Reliability Assurance Initiative, launched by NERC in 2014 and approved by FERC in 2015.[54]

The Reliability Assurance Initiative allows for utility to conduct an inherent risk assessment of each component[55] of the electric utility's system subject to CIP requirements. A higher relative risk would be assigned to those components of the bulk power system whereas a lower risk would be assigned to smaller entities such as renewable and generation providers.[56] The level of self-monitoring is determined by the relative risk level of the component to the system's reliability, with a more expansive degree of oversight applied to those components posing the greatest risks.

Finally, utilities can participate in a voluntary self-evaluation process established by DOE to assess the robustness of their cybersecurity risk management strategies. This process relies on a model, known as the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which constitutes a common set of best practices.[57]

C. Roles of State Public Utility Commissions in Exercising Oversight

While FERC has exercised oversight of BES compliance with its standards, PUCs have also taken concrete steps to improve electric utilities' cybersecurity under their respective jurisdictions. Based on regulatory actions gleaned from providing cybersecurity training and technical assistance to 44 states and other jurisdictions, NARUC's primer identified five actions to improve cybersecurity oversight measures:

- Create expertise within their own organizations;
- Ask the right questions of utilities;
- Assess their own cybersecurity and information protection capabilities;
- Engage with other efforts: led by the private sector, state agencies, or federal agencies, as well as engaging with processes that link these sectors; and
- Assess and improve their cyber strategy.[58]

---

[52] NARUC's cybersecurity primer defines "risk management" as: "the process of conducting a risk assessment, implementing a risk mitigation strategy, and employing of techniques and procedures for the continuous monitoring of the security state of the information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place – synonymous with risk analysis." See Keogh and Thomas, ftn. 15.

[53] NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Last accessed December 4, 2017. An update to the NIST Framework was proposed in January 2017 (Version 1.1).

[54] NERC, "Risk-Based Compliance Monitoring and Enforcement Program," http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx. Last accessed December 11, 2017.

[55] Components required to comply with CIP standards are referred to as "Registered Entities."

[56] James Stanton, "Where Are We After 10 Years of Bulk Electric System Reliability Standards," *Power Magazine*, February 1, 2017, http://www.powermag.com/where-are-we-after-10-years-of-bulk-electric-system-reliability-standards/. Last accessed December 5, 2017.

[57] An explanation of ES-C2M2 is available at: https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity Last accessed December 12, 2017.

[58] Keogh and Thomas, ftn. 15, at 23.

PUCs face many of the same challenges as utilities in attracting and retaining employees with cybersecurity expertise. Commissions compete with utilities for skilled employees with the added disadvantage of inadequate state pay-scales.[59] Staff with the appropriate expertise will be able to explore with utilities various elements of cybersecurity plans.

NARUC's primer (Appendix A) includes questions public utility commissions might ask with respect to cybersecurity planning, standards, reporting, partnerships, procurement practices, personnel and policies, use of risk-management, strategy implementation and impact assessment, response and recovery, general process, governance, and systems and operations.

In addition to steps delineated in the NARUC primer, PUCs have adopted several measures, some formal and some informal, to induce electric utilities to improve their security. According to an article in *Public Utilities Fortnightly*, PUCs have convened stakeholder working groups and have also initiated docketed cybersecurity rulemaking, AMI deployment proceedings, and rate cases that addressed protection and prevention investments. They have also conducted audits and issued reporting requirements.[60]

Not all states leading the way in implantation of the smart grid are focusing specifically on cybersecurity. The GridWise Alliance's Grid Modernization Index benchmarks all 50 states annually in terms of their plans, regulations, and policies, rate structures, and smart technology deployment, considered to be important indicators of smart grid technology policies and deployment. It is therefore perhaps not surprising that the top-ranked states in the most recent survey include California, Illinois, Texas, Maryland, Oregon, Arizona, New York and Delaware, as well as the District of Columbia, because those states are in the forefront of smart grid deployment.[61]

PUCs are instrumental in developing the policy framework for grid modernization. While not cited as a leader in the Grid Modernization Index, Connecticut's Public Utility Regulatory Authority (PURA) has proceeded in a linear manner to implement cybersecurity policy which is integral to grid modernization, by engaging with electric and other regulated sector utilities in efforts to improve cybersecurity. The Connecticut example provides insight into how cybersecurity issues might be addressed at the state level.

[59] Michael Brooks, "After 10 Years, Time to Prune Reliability Standards, FERC Told," *RTO Insider*, June 25, 2017, https://www.rtoinsider.com/ferc-reliability-standards-44953/ [referencing comment by Commissioner Robert Scott of New Hampshire Public Utilities who said, "People with these types of skills are very marketable and they're very mobile. At the state level, we can't hope to attract those (sic) type of people."] Last accessed December 5, 2017.
[60] Edwards *et al*., ftn. 29.
[61] Herman K. Trabish, "As Grid Modernization Accelerates, Which States are in the Lead, and Why?" *UtilityDive,* December 5, 2017,

The table below summarizes the approach Connecticut has taken to that end:

Date	**Action**
February 19, 2013	*Comprehensive Energy Strategy for Connecticut* The report recommended that PURA prepare an unclassified report based on a review of the energy and water sectors' capacity to deter cyberattacks and recommend actions to strengthen their deterrence capacity.
April 14, 2014	*Cybersecurity and Connecticut's Public Utilities* PURA posed questions for utilities to consider in technical meetings. These questions related to performance criteria, the role of the regulator, consistency of state regulation, reporting of cyber threats, information sharing, proprietary practices and best practices, confidentiality, personal security, reporting standards, municipal utility oversight, cost/benefit considerations, and training. PURA also recommended that "Connecticut should consider starting with self-regulated cyber audits and reports and moving toward a third-party audit and assessment system."
May 12, 2014	Opened docket 14-05-12, Cybersecurity Compliance Standards and Oversight Procedures PURA requested input on questions posed in state's 2013 Comprehensive Energy Strategy through discovery and technical meetings, and expressed intent to develop a set of compliance standards and oversight procedures for strengthening cybersecurity.
June 13, 2014	PURA announced its intention to hire a consultant with expertise in cybersecurity.
January 15, 2015	PURA announced a series of collaborative technical meetings, each focused on a utility industry, to define standards for the PURA to use in determining that utility companies are taking steps to strengthen the State's cybersecurity capacity.
April 6, 2016	*PURA Cybersecurity Compliance Standards and Oversight Procedures* The standards and procedures were developed from a series of technical meetings held during 2014 and 2015. Among other things, the final oversight procedure uses voluntary annual meetings of utilities and regulators to oversee compliance activities. Procedure is outside the formal regulatory process. First voluntary oversight reviews were held in early 2017. (See entry for first annual report published in October 2017.)
July 10, 2017	*Connecticut Cybersecurity Strategy* The Governor supported the PURA compliance and oversight procedures initially implemented in 2017.
October 12, 2017	*Connecticut Critical Infrastructure 2017 Annual Review Report* The annual review report described in general the voluntary oversight process and identified in general terms challenges and areas of progress, and identified the need for participation of municipal utilities, cooperative utilities, and broadband and cable providers in the annual reviews.

The PURA approach had its genesis in a comprehensive state-wide cybersecurity initiative of the Governor. Development of utility cybersecurity oversight standards and procedures began with a series of technical meetings between PURA and electric and gas public utilities. During those meetings participants reviewed then-current standards and guidelines of the utilities' cybersecurity risk management programs. An essential component of the Connecticut approach growing out of those original meetings centered on voluntary collaboration and cooperation between utilities and PURA. Once standards were developed, oversight was to be implemented through annual meetings involving the PURA and the state Division of Emergency Management and Homeland Security. During these annual meetings, the utilities are expected to report on their cyber defense programs, prior year experiences related to cyber threats, and proposed corrective measures for the following year. PURA's Cybersecurity Oversight Program reporting requirements limit cybersecurity review meetings to once a year and make it clear that utilities need not submit formal, written reports. The report of each oversight meeting is provided to the Governor and the General Assembly.[62] A voluntary oversight program such as Connecticut's may be applicable to public and cooperative utilities not generally subject to regulation by a PUC.

Delaware took a slightly different approach. The Delaware Public Service Commission opened a docket to review the necessity for cybersecurity guidelines or regulations. After reviewing what utilities had undertaken in terms of internal guideline development and implementation and their plans to stay abreast of evolving technologies, the staff concluded that guidelines and standards were unnecessary at that time. Based on staff's recommendations, the Delaware Commission ordered its utilities to respond to a list of cybersecurity questions and directed Commission staff to conduct an annual review of those responses. Annually, the questions will be posted on the Commission's website and utilities are required to respond to them within 30 days of posting.[63]

Yet another approach to regulatory oversight is the establishment of standards and guidelines such as Michigan's order for the promulgation of rules that would provide for:

- an annual report that includes an overview of the electric or gas provider's cybersecurity program;
- a list of the company's cybersecurity departments, staffing numbers and position descriptions, and the names of key contacts;
- a description of any cybersecurity training and exercises undergone by employees;
- an explanation of any cybersecurity investment made and the rationale for such investment;
- a discussion of the tools and methods used to conduct risk and vulnerability assessments; and

[62] Arthur H. House, Chairman and Stephen M. Capozzi, Lead Staff, *Connecticut Public Utilities Cybersecurity Action Plan.* Connecticut Public Utilities Regulatory Authority, Docket No. 14-05-12, PURA Cybersecurity Compliance Standards and Oversight Procedure, April 6, 2016, 2 and ftn. 1, http://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf. Last accessed December 5, 2017.

[63] Delaware Public Service Commission, *In the Matter of the Commissions' Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Investor Owned Electric, Gas, and Water*, PSC Docket No. 16-0659, Order No. 8955, May 23, 2016. Questions posted are found in Exhibit A of the order.

- a summary of cybersecurity incidents that resulted in a loss of service, financial harm, or a breach of sensitive business or customer information.[64]

Perhaps the most hands-off approach, adopted in Pennsylvania, is a requirement for utilities to self-certify that they have cybersecurity plans that are subject to PUC audits.[65]

Several general questions regarding process, procedure, and implementation were highlighted in these states' experiences.

D. Questions and Trade-offs for Public Utility Commissions and Challenges for the Future

In its 2014 strategic plan Connecticut's PURA recognized that there was no "quick fix" solution to ensuring protection against cyberattacks and that the work is evolving and ongoing: "This serious work has just begun and will evolve in the years to come. Connecticut should approach cybersecurity for its public utilities in terms of phased work: efforts that are continually examined and improved upon. As we learn, we must adjust. As we understand, we must update, improve and build better defenses."[66]

As threats continue to evolve, each PUC will need to proceed with its oversight activities based on its own regulatory and legal framework. Connecticut's efforts, NARUC's experiences with state PUCs' strategies, and issues raised in the sources reviewed for this paper can be distilled into policy questions for PUCs and other policymakers to consider as they proceed with their cybersecurity planning and response efforts:

1. Does the PUC have statutory authority to access and use sensitive utility security-related data with guaranteed confidentiality for the utility?

   Without such access and guaranteed protection, PUCs may be impeded from making prudent cost recovery decisions and exercising other aspects of oversight related to utility service. Fairly typical are statutes such as those of Connecticut which provide confidentiality protections to certain information supplied to the PUC by a utility.[67]

2. What must the PUC do to facilitate the sharing of sensitive information and how will customers be protected in the process? Also related to information sharing, what must be done to ensure that both utility officials and PUCs have sufficient security clearances to be able to receive classified information from national security officials who are also monitoring the security of critical infrastructure? While maintaining confidentiality of security information is crucial, implementation

[64] Michigan Public Service Commission, *In the matter, on the Commission's Own Motion to Review Issues Concerning Cybersecurity and the Effective Protection of Utility Infrastructure*, Case No. U-18203, Order, November 22, 2016, 3. https://www.michigan.gov/documents/mpsc/u-18203-11-22-2016_565207_7.pdf. Last accessed December 5, 2017.

[65] Pennsylvania Utility Commission, *Public Utility Security Planning and Readiness Self-Certification Form*, Revised November 29, 2016, https://www.puc.state.pa.us/general/onlineforms/pdf/Physical_Cyber_Security_Form.pdf. Last accessed December 5, 2017. Authorization for plan and self-certification in Public Utility Code, 66 Pa.C.S. §101.1-7.

[66] Public Utility Regulatory Authority (PURA), *Cybersecurity and Connecticut's Public Utilities*, 25. http://www.governor.ct.gov/malloy/lib/malloy/2014.04.14_pura_cyber_report.pdf. Last accessed December 11, 2017.

[67] Connecticut Statutes 16-8c(c). Exemptions to the "Access to Public Records" statute in Sec. 1-210 (b) (5).

of effective cybersecurity measures involves participation of multiple entities and tends to involve multiple types of infrastructure (electricity, telecommunications, water, natural gas). The ability to share sensitive utility and customer-related data among partners in a secure and timely manner is equally important.

3. How safe is safe?

The CIP standards are compulsory, but many industry standards are voluntary, such as NIST's cybersecurity standards and DOE's ES-C2M2. Moreover, most federal or nationally-developed standards and processes apply to the BES. The PUC is faced with the questions of cybersecurity not necessarily subject to CIP so additional security measures may be necessary.

All compliance and risk management measures have associated costs. How might PUCs think about the trade-off between compliance and risk management costs and potential benefits to adoption of compliance and risk management measures? Additionally, how do PUCs encourage utilities to think and act beyond compliance to reach effective risk management for the system?

It is intuitive that not all risks can be eliminated completely because adversaries adapt to defensive changes made to the electric grid so the challenge to utilities is to set priorities. Appropriate incentives will be needed to encourage utilities to adopt strategies that include priorities for the most important processes and infrastructure needed to protect against attacks.[68] For their part, PUCs need to understand those strategies and make sure that, to the extent they have any control in the matter, incentives are aligned to promote their adoption.

4. Assuming PUCs have the requisite authority to access the utility's cybersecurity-related expenditure data, what is the optimal cost recovery mechanism to encourage electric utilities to effectively manage risks against cyber threats?

Cost recovery of electric utility cybersecurity investments may be problematic for utilities to justify to PUCs because they potentially compete with investments needed for more traditional types of emergencies such as outages from storms. Even if proposed investments do not compete, certain items like redundant or mirrored systems,[69] might be hard for commissions to justify given the uncertainty of emergency incidents.[70]

Cost recovery for cybersecurity measures can be approved as part of traditional rate cases. For example, Connecticut's investor-owned electric utility, Eversource, recently announced that it is seeking a rate increase of 6.79%. As part of its justification, the utility referred to its investments in

[68] Michael Assante, Tim Roxey, and Andy Bochman, *The Case for Simplicity in Energy Infrastructure For Economic and National Security*, Center for Strategic & International Studies, October 2015, 7, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf. Last accessed December 5, 2017.

[69] A growing concern is that utilities' complex systems do not enable them to easily resort to manual control of operations in an emergency. The less complex system in Ukraine that was able to switch to manual control helped mitigate the attack against Ukraine's power grid. A possible risk management measure would be to require utilities to develop the capacity to shift to manual control of operations and exercise those controls annually. The utility should ideally have backup operational tools that are isolated from the grid or are analog. See Knake at ftn. 1.

[70] Edwards *et al*., ftn. 29.

"advanced technology solutions to protect the electric grid from cybersecurity threats," which were intended to enhance reliability for its customers.[71]

Finally, an argument can be made that utility investments in cybersecurity should yield the greatest benefit for improving safety in order to justify cost recovery. An article in *Public Utilities Fortnightly* described an economic theory suggested by economist Ken Costello that was used for cost allocations to improve natural gas pipeline safety. The idea is that there is no 100% guarantee of safety, so a utility should strive for incremental measures which yield the most benefit. If too much money is spent on safety for low risk protection, an opportunity to allocate the investment elsewhere is forgone.[72]

5. How should a PUC best position itself to assess the utility's cybersecurity preparations?

Utilities typically pay more than PUCs for technical staff, such as those with cybersecurity expertise. If utilities have difficulty attracting such employees, it will not be surprising that PUCs cannot compete. Indeed, a commissioner of the New Hampshire PUC observed: "At the state level, we're generally not staffed for this type of thing. We don't have the expertise."[73]

For its part, the Connecticut's PURA recognized it lacked the skill sets to competently work with jurisdictional electric utilities in technical cybersecurity meetings, so it contracted with a third party, Applied Communications Sciences to obtain necessary expertise. In situations where third party expertise is involved in security analyses, additional complexity is created regarding information sharing.

6. What standards, plans, and procedures do states have in place to facilitate rapid recovery from a cyber-incident that disrupts utility service? Are those procedures compatible with existing regional and national cyber incident response procedures, including forensic investigation procedures? Do the designated state, regional, and federal officials responsible for response have effective joint action and communication protocols?

The challenge for PUCs is to encourage electric utilities under their jurisdictions to improve their responsiveness in a manner in which benefits exceed costs since every compliance requirement will exact some cost on the utility. A National Academy of Sciences (NAS) report includes a recommendation that envisions PUCs playing a role in preparing their states and regions for long-term blackouts. The recommendation acknowledges the need for interagency cooperation:

> Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments

[71] Wilton Bulletin, "Eversource Pursues Rate Increase," *Wilton Bulletin com,* October 30, 2017, https://www.wiltonbulletin.com/109955/eversource-pursues-rate-increase/. Last accessed December 5, 2017.
[72] Edwards *et al*., ftn. 29.
[73] Brooks, ftn. 59.

to conduct assessments of their potential vulnerabilities in the event of large-area, long-duration blackouts and to develop strategies to improve their preparedness.[74]

That same report recommends that PUCs and other stakeholders explore compensation mechanisms for owners of distributed energy resources who are able to dedicate a portion of their generation capacity to serve as "islanded feeders" in the event of long-duration outages.[75] In many states, that issue of compensation could be complicated by the regulatory structure governing DERs.

Although methods may vary, PUCs need to know what jurisdictional electric utilities are doing to prepare for recovery from cyber incidents. Connecticut's PURA provides one approach. Recovery was a subject of discussion during the first annual review in 2017. In the report of that review, PURA summarized utility actions to both strengthen deterrence and recovery efforts. The review also outlined areas of concern, such as better coordination with law enforcement and investigation at the state level.[76]

7. What role should PUCs play in ensuring that customer data breaches are quickly and appropriately addressed, leaks stopped, and consumers protected from adverse consequences? Do PUCs have a role in enforcing state cybersecurity laws involving breaches of third parties doing business with regulated utilities?

Some PUCs exercise oversight of third-party data breaches. For example, the New York Public Service Commission took several actions that culminated in a decision to review every jurisdictional large utility's data security policies and procedures. These actions were spurred by the discovery that an employee of one of the utilities (NYSEG) had improperly shared log-in credentials with subcontractors, thereby disclosing sensitive information affecting 1.8 million customers.[77]

PUCs can exercise direct oversight over non-utilities or third-parties that disclose customer data improperly if the commission has appropriate authority. There is no federal policy establishing how access to customer data should be treated so the issue is almost solely governed by state statutes and commission actions. For example, the California Commission determined it had such authority based on a court decision, *PG&E Corp. v. Public Utilities Com*. (2004) 118 Cal. App. 4th at 1174. The Commission also determined that state law grants it that authority. The rules promulgated by the California Commission on the privacy and security of electricity usage data reflect its authority to act against third parties that disclose customer information improperly. [78]

---

[74] *Enhancing the Resilience of the Nation's Electricity System*, ftn. 15, 7-6/7.

[75] Ibid., 5-26.

[76] PURA, *Connecticut Critical Infrastructure 2017 Annual Review Report*, 6.

[77] New York State Public Service Commission, "PSC Tells NYSEG. RG&E to Improve Consumer Safeguards — Investigation into Security Breach of Consumer Information Spurs Call for Change," Press Release, July 12, 2012, http://www3.dps.ny.gov/pscweb/WebFileRoom.nsf/Web/5772136EE27214FA85257A3900615AA2/$File/pr12059.pdf. Last accessed December 5, 2017.

[78] California Public Utilities Commission, *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company*, Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System, July 28, 2011, http://docs.cpuc.ca.gov/published/final_decision/140369.htm#P244_46555. Last Accessed December 5, 2017.

8. Do PUCs have a security role to play in protecting the network, utility assets, and consumers when it comes to non-utility smart grid systems, applications, devices, and entities have access to the electricity network?

While PUCs do not currently regulate non-utility smart grid systems, one-way PUCs can address risks created by the smart grid is to support development of interconnection standards for devices much as standards have evolved for customer-generated power and other distributed generation. The authors of the NAS report recommend specifically that PUCs ". . . work closely with operating utilities to assess their current interconnection standards as applicable to DERs . . . consider the costs of requiring new installations to use enhanced inverters, and determine the appropriate policy for promoting islanding and other related capabilities."[79] NARUC's primer suggests questions PUCs may pose to utilities regarding smart grid technology as it relates to procurement practices and to the integration of smart grid systems with the utility's business and control systems [80]

Microgrids, both publicly-owned and privately-owned, are becoming a more common way to improve resilience of the grid during power outages and for potential contributions to reliability. For example, a recent report titled "Enhancing the Resilience of the Nation's Electricity System" recommends that: "State legislatures and public utility commissions should explore economic, ratemaking, and other regulatory options for facilitating the development of private microgrids that provide resilience benefits. Rate structures can be developed to cover the costs of upgrading and maintaining grid assets while also recognizing and rewarding the benefits that distributed energy resources provide to the grid."[81] As in the evolving arena of distributed generation, creative policy making will be necessary to secure the grid as it encompasses territory outside the fence and far afield from the easement around the line.

E. Final Thoughts

Some of the questions raised here for consideration of PUCs can only be resolved during public policy debate among lawmakers and other stakeholders in each state. Clearly, members of PUCs are in a unique position to contribute to the development and maintenance of cybersecurity policies for state government and a large segment of critical infrastructure. While the focus of this paper is on cybersecurity of the electric system, PUCs may have an equally important role in providing expertise and perspective to policies supporting cybersecurity of the telecommunications network, in its varied technological manifestations. The integration of communication technology in the smart grid and in aspects of the automated operation of the electric grid along with the business side of utilities puts PUCs in a unique position to make significant contributions to development of holistic cybersecurity laws, regulations, and standards in the states. Further, the interconnection of IOUs, co-ops, and publicly-owned utilities regulated at different levels and for different purposes may in some cases create a level of vulnerability to the grid. Sorting out the

[79] *Enhancing the Resilience of the Nation's Electricity System*, ftn. 15, Recommendation 5-7, at 5-24.

[80] The questions are: Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity, and website hosting? Is cybersecurity integrated between business systems and control systems? For the existing grid and for the smart grid? See Keogh and Thomas, ftn. 15, Appendix A.

[81] *Enhancing the Resilience of the Nation's Electricity System*, ftn. 16.

appropriate role of PUCs vis-a-vis cybersecurity issues as those issues pertain to less traditionally regulated utilities also may require reshaping state laws.

Protection of the grid may necessitate PUCs being charged with responsibilities outside the usual range of concerns about reliable, affordable power because the availability of electricity is integral to every function of society including defense and recovery, as the country has learned from Puerto Rico's arduous experience. Moreover, the interconnection of systems used to operate and secure the modern electrical grid may create the need for a different type of cost-benefit calculus than that traditionally considered for utility cost-recovery applications.

Acknowledgements: The authors wish to thank Allan Foster for his thoughtful review and suggestions on an earlier version of this paper.