A Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues

Daniel Phelan
Research Associate
National Regulatory Research Institute

Report No. 14-12
December 2014

8611 Second Avenue, Suite 2C
Silver Spring, MD 20910
Tel: 301-588-5385
www.nrri.org

National Regulatory Research Institute

About NRRI

NRRI was founded in 1976 by the National Association of Regulatory Utility Commissioners (NARUC). While corporately independent, NARUC and NRRI are linked in multiple ways to ensure accountability. NARUC, as the association of all state regulators, is invested in quality research serving its members. NRRI coordinates its activities to support NARUC's policy, research, educational and member-support service to state commissions.

Mission Statement

To serve state utility regulators by producing and disseminating relevant, high-quality research that provides the analytical framework and practical tools necessary to improve their public interest decision-making. In all its activities, NRRI embodies the following values: relevance, excellence, objectivity, creativity, independence, fiscal prudence, ethics, timeliness and continuous improvement.

Board of Directors

Acknowledgments

The author would like to thank the members of the Middle Atlantic Cybersecurity Collaborative (MACC) for their input and continued feedback on this report. **Commissioner Joanne Doddy Fort** (District of Columbia PSC), **Commissioner Asim Haque** (PUC of Ohio), **Commissioner Ann Hoskins** (Maryland PSC), **Chairman Kevin Hughes** (Maryland PSC), **Chairman Betty Ann Kane** (District of Columbia PSC), **Chairman Robert Powelson** (Pennsylvania PUC), **Commissioner Dianne Solomon** (New Jersey BPU), **Chairman Dallas Winslow** (Delaware PSC), and **Commissioner Pamela Witmer** (Pennsylvania PUC) provided excellent insight into the cybersecurity procedures of state utility commissions. A special thanks to **Commissioner Witmer** who was designated as the lead commissioner for MACC. Additionally, input from several MACC staff members – **Lois Burns** (Pennsylvania PUC), **Thom Pearce** (PUC of Ohio), **Ron Teixeira** (Delaware PSC), and **Ellen Vancko** (Maryland PSC) was essential in compiling this report.

Beyond MACC, **Chairman Robert Kenney** (Missouri PSC), **Pat Poli** (Michigan PSC), **Doug Chapman** (Midcontinent Independent System Operator), **Steven Greenlee** (California Independent System Operator), **Laura Koepnick** (Massachusetts Department of Public Utilities), **Steve McElwee** (PJM Interconnection), and **John Sennett** (New York State Department of Public Service) offered valuable insight from their respective organizations' experiences and practices.

The author would also like to thank his colleagues at NRRI – **Ken Costello, Rishi Garg,** and **Sherry Lichtenberg** – for their input on the draft versions of this report. Finally, the author thanks **Rajnish Barua** for his guidance, coordination, and support throughout this project.

About the Author

Daniel Phelan is Research Associate at NRRI and joined NRRI in December 2012. Previously, Mr. Phelan worked as in the office of former U.S. Senator Scott P. Brown. Mr. Phelan has also worked in several political campaigns in New England. His current major assignments at NRRI include conducting directed research and assisting all NRRI's researchers with their background research. In June 2014, he authored NRRI Briefing Report No. 14-04, *A Primer on the Status of the Keystone XL Pipeline Project.* He earned his bachelor's degree from the University of Vermont as a Political Science major with a minor in Business Management.

Executive Summary

The United States' critical infrastructure sectors face the risk of cyber attacks on a frequent basis, with potential impacts that could cause damage to vital systems, expose customer information to theft, or severely limit necessary safety activities. To get a better understanding of those issues, the Middle Atlantic Cybersecurity Collaborative (MACC)[1] directed the National Regulatory Research Institute (NRRI) to study the cybersecurity responsibilities and practices of state utility commissions across the nation as well as the roles of numerous other state, federal, and private sector organizations.

This study describes the relationship of cybersecurity issues to some basic commission responsibilities and the associated challenges in cybersecurity regulation. Then, the study compiles actions taken by various commissions, including ongoing dockets that may result in further rules or orders, and how cybersecurity expenses have been treated within some rate cases. The study then examines actions taken by other organizations such as federal agencies, state legislatures, and industry organizations, and concludes by identifying trends in state utility commission actions.

One of the prime responsibilities of a commission is to ensure safe and reliable service. A cyber attack represents a threat to the system reliability of each utility sector, and could impact a system in a number of ways. Furthermore, the integration of utility systems has wide-reaching effects on public health and safety; i.e., without electricity, communications systems, gasoline pumps, water purification systems, and other utility systems would not be able to function. Each utility sector offers invaluable support to other utility sectors, and the cascading effects of a cyber attack would be extreme. While each attack can have a different target and method, they ultimately impact system reliability and customer service.

Utilities hold and store valuable customer information, including financial information, usage data, and physical information. Information systems have the ability to efficiently store this data and provide utilities the ability to offer innovative new services. However, they also create risk for ratepayers. The breach of a utility's information technology systems, the standard networks used to complete business processes, could allow access to customer information, business practices, or security information related to control systems. A utility operating these systems without consideration for cybersecurity opens its ratepayers to dangerous cyber attacks, including identity theft and the compromise of privacy.

Commissions ultimately have a responsibility to allow cost recovery of prudent expenses within just and reasonable rates. All utility ratepayers benefit from prudent cybersecurity measures due to their impact on reliability, safety, and consumer protection. Utilities are therefore entitled to recover the cost of prudent cybersecurity expenses from their rate-base.

---

[1] MACC is group of commissioners and staff from the following Mid-Atlantic commissions: Delaware PSC, District of Columbia PSC, Maryland PSC, New Jersey BPU, PUC of Ohio, and Pennsylvania PUC (see Appendix A).

Commissions are responsible for assessing a utility's cybersecurity expenses, and ultimately allowing those prudent expenses.

Given these responsibilities, commissions must ensure that their regulated utilities are ready to face cybersecurity threats. However, some challenges arise when a commission examines cybersecurity. Jurisdiction can challenge a commission in multiple ways. A regulated utility may have a service territory reaching beyond the jurisdiction of just one commission, creating compliance requirements with multiple, varying cybersecurity regulations. Further, federal agencies share cybersecurity responsibilities, muddling jurisdictional lines. While the Bulk Electric System falls under the purview of the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) regulations, it has been estimated that 80%-90% of grid assets are outside the scope of the CIP standards. Each utility sector reports to a different federal agency; e.g., the Environmental Protection Agency, Transportation Security Administration, Department of Energy, and Federal Communications Commission each govern a specific utility sector. The Department of Homeland Security ultimately coordinates communication across sectors, but between competing state regulations and federal agencies, it is often difficult for a state commission to clearly understand where jurisdictional lines are drawn.

Liability concerns also create a significant risk for a utility. Utilities may be hesitant to participate in valuable information sharing resources because they may be concerned about being held responsible for cybersecurity attacks that they were told about. In the past, companies have faced legal action from the Federal Trade Commission, state attorneys general, and shareholders in the aftermath of a cyber breach. Utilities may be hesitant to undertake necessary cybersecurity expenditures without guarantees of liability protection or cost recovery.

When a state commission examines cybersecurity expenses, it can also face difficulty coping with confidentiality challenges. Cybersecurity measures necessitate a degree of secrecy, both in defense practices and incident response plans. Unless properly shielded by clearly defined statutory protections, requests under the Freedom of Information Act made to a commission may expose the details of a utility's cybersecurity plan. Utilities may be hesitant to even provide this information to commissions, despite the fact that commission must have this information in order to assess the prudence of an expense. Conversely, in many states, information received by state employees may be deemed to be public information and, therefore, again risking the exposure of critical details.

Another associated challenge is that of technical knowledge. Once each of these previous challenges has been addressed, commissions must have the technical knowledge to understand what does or doesn't make a prudent investment. A utility's cybersecurity expenses may have been imprudent even if an attacker does not breach their systems, and even prudent expenses cannot be assured to prevent all cyber attacks. Familiarity with at least the basic details of cybersecurity is needed within a commission to fully evaluate a utility's plans.

With those responsibilities and challenges in mind, commissions have reacted and begun to formulate their cybersecurity policies. Eleven state commissions have concluded dockets with rules or orders that focused on cybersecurity. Some commissions have asked their utilities questions about their cybersecurity plans, usually with considerations for confidentiality, while some commissions have addressed cybersecurity within the topic of smart meters, or as a

condition of Advanced Metering Infrastructure (AMI) rollouts. Other commissions have said that cybersecurity is a safety and reliability issue, and have developed planning or reporting requirements. There are currently 11 open dockets in separate jurisdictions that address cybersecurity issues. These largely tend to include cybersecurity considerations within AMI rollouts. These open dockets also address third party access to customer data, cost recovery of expenses related to NERC CIP, and the development of an extensive cybersecurity plan.

Commissions have also attempted to bridge the gap in technical knowledge. Programs conducted by the Department of Homeland Security and the National Association of Regulatory Utility Commissioners have involved 19 and 37 commissions, respectively. Commissions have also had meetings and briefings with their regulated utilities. Frequently, there is little or no record of these discussions, due to confidentiality concerns, but details of a utility's cybersecurity plans are shared with its jurisdictional commission.

Cybersecurity has been directly mentioned within rate cases. Traditionally, cybersecurity expenses have been recovered as part of larger system costs. Utilities have included cybersecurity considerations within their equipment evaluations, and then sought recovery for the entirety of the system cost. However, increased scrutiny on cybersecurity has drawn more discussion into general rate cases. In seven states, utilities have explicitly detailed cybersecurity costs within one or more rate cases. In roughly half of these cases, the utility has described the costs as regulatory compliance with NERC CIP or Nuclear Regulatory Commission requirements. Cybersecurity costs have also been included within capital additions, operations and management, and information technology costs. In these cases, utilities identified cybersecurity as a driving factor in cost increases within larger categories.

Actions taken by state utility commissions must fit within the larger regulatory environment, which includes federal agencies, state legislatures, and private industry organizations. Since President Clinton's administration, each president has taken steps to improve the United States' cybersecurity measures. Each utility sector is responsible to a separate federal agency, with the Department of Homeland Security coordinating between all public and private actors. Nine state legislatures have passed legislation addressing cybersecurity in relation to AMI or creating a cybersecurity coordinator within the state. Industry organizations also offer guidance to their member utilities through a variety of standards and resources.

State utility commissions therefore have a number of questions to ask themselves before developing cybersecurity standards. While cybersecurity regulation is young and "best practices" have yet to be examined and developed, commissions can develop regulations by asking themselves about the confidential treatment of security information, the responsibilities they may have been given by their state legislatures, the availability of training programs, the opportunities available for their staff to participate in cybersecurity information-sharing initiatives, and other questions identified in Section 6 of this report.

Table of Contents

List of Tables

Introduction

The prevalence of advanced communications technologies allows utilities to implement new controls and offer innovative services to their customers. Utilities use a variety of industrial control systems (ICS) to monitor and control their infrastructure, and these ICS have become increasingly connected by information networks. However, the implementation of these systems introduces vulnerabilities with which utilities and utility regulators likely are unfamiliar. Electric, water, oil, natural gas, and telecommunications companies all face cybersecurity threats to public safety and the integrity of customer information. The critical infrastructure regulatory community must consider actions to ensure the security of these information networks from a wide variety of threats.

Several organizations have therefore created cybersecurity standards, which have largely taken the form of voluntary guidelines. Cybersecurity experts have emphasized voluntary standards so as to avoid a mere minimal level of compliance, and note that even a regulatory requirement for cybersecurity procedures would not eliminate the risk of cyber threats. Still, many government agencies are looking to do more to ensure the protection of America's critical infrastructure. State utility commissions[2] have begun to explore their roles in this regulatory environment.

In general, state regulators are charged with ensuring that utilities provide safe and reliable service at just and reasonable rates. Cybersecurity falls under the purview of state utility commissions because breaches can negatively impact system reliability, the cost of service, and the protection of ratepayers' private information. Yet, overseeing cybersecurity presents new challenges to commissions. Traditionally, cybersecurity expenditures have been recovered as part of regular utility expenses without special consideration. As cybersecurity becomes a larger focus for commissions, jurisdiction, liability, confidentiality, technical knowledge, and the development of new technologies distinguish cybersecurity from other expenditures and thereby complicate the regulatory role. Various state commissions have adopted new rules and regulations; expanded commission and commission staff knowledge of cybersecurity; held meetings and briefings with regulated utilities; and continue to develop rules through ongoing regulatory proceedings.

State utility commissions are not acting alone in this field. The federal government has, through several laws and various agencies, created many cybersecurity standards, guidelines, and programs. State governments have also passed legislation encouraging the consideration of cybersecurity in "smart grid" development, focusing on improving the information sharing process between the private and public sector, and addressing the regulatory process. Finally, utility trade groups/associations have developed sector-specific guidelines for multiple areas of

---

[2] Throughout this paper, the terms “commissions” and “regulators” are used interchangeably and represent the individual statutory/constitutional agency that regulates monopoly utility services in each of the 50 states and the District of Columbia.

focus, including specific practices for each of the electric, water, natural gas, oil, and telecommunications sectors.

The Middle Atlantic Cybersecurity Collaborative (MACC) [3] requested that the National Regulatory Research Institute (NRRI) conduct a study of commission, legislature, and other organization cybersecurity responsibilities and practices. This report examines how state commission responsibilities relate to cybersecurity, reviews the challenges these commissions face in developing cybersecurity regulations, and relates actions that commissions have already taken. The report also details the variety of cybersecurity actions taken by the federal government, state legislatures, and utility organizations. Finally, the report identifies trends for state utility commissions considering implementing or improving cybersecurity policies.

Commission Responsibilities

While cybersecurity is a new field of focus for regulators, it fits within the traditional role of regulation. State utility commissions largely share similar responsibilities, despite differences in authorities. Commissions typically have oversight responsibilities for customer protection, reliability and safety of service, cost recovery of prudent investments, and to ensure just and reasonable rates. Cybersecurity raises challenges for each of these areas that commissions will need to address going forward. This section describes the major responsibilities of state utility commissions, and explains how each of those responsibilities relates to cybersecurity.

1.1. Reliability and Safety

State utility commissions have a responsibility to ensure the reliability and safety of service. A cybersecurity event, in which a utility's ICS or other information technology networks are breached by unauthorized users, could result in widespread service interruptions from which it could be difficult to recover. Researchers and attackers have already demonstrated the ability to disrupt or permanently damage essential utility system components. Public health and safety are threatened by extended electric outages, contamination of water resources, disruption of gas pipelines, or other unforeseen impacts.

Every utility, no matter the size, faces a threat from cyber attacks. Smaller companies without the financial resources of a large company may be at a greater risk to withstand legal action or the reputational consequences of a cyber attack. With the integrated nature of the United States' utilities, an attack on a small utility can have far-reaching, cascading repercussions. No utility should find itself to be exempt from cybersecurity measures due to the broad-reaching reliability and safety impacts a cyber event could cause.

Cyber attacks on any utility could have impacts on other utilities in different sectors. The integration of utility systems has wide-reaching effects on public health and safety: without electricity, for example, communications systems, gasoline pumps, water purification systems,

---

[3] See Appendix A for the resolution text and a list of Middle Atlantic Cybersecurity Collaborative members.

and other utility systems would not be able to function. Each utility sector offers invaluable support to other utilities, and the cascading effects of a cyber attack would be extreme.

A cyber attack could affect a utility in a number of ways. Water and wastewater utilities could see interference with water treatment leading to improper chemical usage; changes to programmed instruction causing disabled service, altered water pressure, or overflow of sewage; or an alteration in alarm thresholds signaling intrusion or contamination.[4] The Stuxnet attack, perhaps the most high-profile cyber attack thus-far, modified code in Programmable Logic Controllers (PLCs) to destroy 1,000 centrifuges in an Iranian nuclear fuel enrichment plant.[5] The Shamoon malware attack on Saudi Aramco, Saudi Arabia's oil company, wiped data from roughly 30,000 computers.[6] While each attack can have a different target and method, they ultimately impact system reliability.

For this reason, commissions should approach cybersecurity events the way they approach extreme weather events, with advanced planning, recovery plans, and testing. The exact circumstances of the next storm or attack cannot be predicted, but the impact can be planned for and mitigated. Incident response plans are important to have in place well before they are needed in order to limit an event's impact on service reliability and public safety.

1.2. Consumer Protection

Utilities hold and store valuable customer information, including financial information, usage data, and physical information. Information systems have the ability to efficiently store this data and provide utilities the ability to offer innovative new services. However, they also create risk for ratepayers. The breach of a utility's information technology systems, the standard networks used to complete business processes, could allow access to customer information, business practices, or security information related to control systems.[7] A utility operating these systems without consideration for cybersecurity opens its ratepayers to dangerous cyber attacks, including identity theft and the compromise of privacy.

Still, these information systems will continue to offer increasingly useful services to utilities and customers. Advanced Metering Infrastructure (AMI) offers utilities the opportunity to better manage system peaks, defer or avoid building infrastructure, and reduce cost to customers. AMI deployment may allow utilities to better integrate renewables, reduce costs to consumers, and provide new opportunities for third party service providers. In order to provide these benefits, AMI offers unprecedented access to customer usage information. A customer's usage habits are highly personal, and unauthorized access to this information would be a serious breach of consumer protection standards. State legislatures and commissions in California,

---

4 United States Environmental Protection Agency, 2008

5 Albright, et al., 2011

6 Clayton & Segal, 2013

7 Keogh & Cody, 2013

Maryland, Maine, and other states[8] have recognized this danger, and have taken steps to ensure the security of smart grid data.

1.3. Cost Recovery and Just and Reasonable Rates

State utility commissions are also tasked with weighing a utility's investment needs with just and reasonable rates. A utility commission allows prudent expenses in reliability efforts to be recovered from ratepayers. All utility ratepayers benefit from prudent cybersecurity measures due to their impact on reliability, safety, and consumer protection. Utilities are therefore entitled to recover the cost of prudently undertaken cybersecurity expenses from their rate-base. Commissions are responsible for assessing cybersecurity expenditures, and ultimately allowing the prudent expenses.

Cybersecurity expenses may arise in two main ways: when included in newly installed systems or added to older systems. Typically, when cybersecurity costs are assessed for new systems, the cost of cybersecurity is not explicitly considered. It is instead included within the cost of the new system. A utility's procurement process will, in most cases, treat cybersecurity as one of many considerations. Adding cybersecurity features to older systems may cause a utility to incur additional expenses beyond what previously was expected or approved by a commission. Cybersecurity might simply not have been a consideration, by either the utility or the commission, when the system was originally installed. Still, cybersecurity is now an important issue for utilities. Cybersecurity policies and procedures should not neglect older systems, and the recovery of costs associated with retrofitting these systems is relevant to commission actions.

Challenges

While attempting to address cybersecurity, state utility commissions have encountered a number of challenges. These issues complicate the regulation of cybersecurity by challenging commission jurisdiction, raising questions of liability, potentially exposing confidential information, asking for new areas of technical knowledge, and challenging commission knowledge of developing technologies.

Combating cyber threats requires a constantly evolving approach, as vulnerabilities are continually being discovered. A secure system today offers no guarantee of a secure system tomorrow, and attackers of varying sophistication frequently test the effectiveness of cybersecurity systems. Utilities and commissions alike have been tasked with rapidly developing knowledge in a critically important area in which they may have little or no experience. Further, the constant evolution of the field requires ongoing monitoring.

It is commonly believed that utility regulation takes the form of a "regulatory patchwork," with each state, and the federal government, having its own rules and priorities.

---

[8] These actions are further discussed in Sections 4 and 5. Other states that have addressed this issue include Illinois, Oklahoma, Texas, and Washington. The District of Columbia, Kentucky, and New York also have ongoing dockets examining cybersecurity within the context of AMI deployment.

Cybersecurity regulations reflect this, and present a complicated regulatory environment. There is no uniform state or federal regulatory scheme for utilities regarding cybersecurity. Regulation also cannot prescribe a single, catchall solution for cybersecurity. Utilities must have the flexibility to apply solutions specific to their needs, and rigid regulation may not allow a utility to adequately respond to a new, dynamic threat. At the most fundamental level, however, cybersecurity presents challenges that fall under the purview of state utility commissions, and commissions must ensure that their regulated utilities are prepared to face these new threats. Commissions, state legislatures, and the federal government must take care to strike a balance between required regulation and flexibility.

1.4. Jurisdiction

Jurisdiction challenges a state utility commission in a number of ways. A regulated utility may have a service territory reaching beyond the jurisdiction of just one commission, causing a single utility to comply with multiple, differing cybersecurity regulations. Cyber attacks may come from foreign nations, far beyond the purview of state regulators. Further, a large number of federal agencies share responsibility for different aspects of cybersecurity. Between competing state regulations and federal agencies, it is often difficult to clearly understand where jurisdictional lines are drawn.

The bulk electric system is under the purview of the Federal Energy Regulatory Commission (FERC), and is subject to the North American Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP) standards. However, local distribution is not regulated by FERC. The California Public Utilities Commission has estimated that 80 to 90 percent of grid assets fall outside of the CIP standards' scope.[9] Instead, state regulatory commissions hold responsibility for cybersecurity local distribution systems. If a utility serves multiple states, it may need to have different cybersecurity policies for different assets, depending on variations in state regulations.

Many federal agencies have jurisdiction over critical infrastructure cybersecurity. Each utility sector falls under a different federal agency: the Environmental Protection Agency oversees water, the Transportation Security Administration oversees pipelines, the Department of Energy oversees electric power and oil and gas production and storage, and the Federal Communications Commission oversees telecommunications.[10] The Department of Homeland Security coordinates communication between these, and other, federal agencies, but there is no singularly responsible federal entity for cybersecurity.

1.5. Liability

Liability presents a significant risk for utilities. Despite the best efforts of utilities and commissions, cybersecurity breaches are possible. Utilities are wary that, in the case of a cybersecurity event, they may be held responsible for damages despite having taken actions to

---

[9] Malashenko, Elizaveta et al., 2012

[10] Clinton, 1998

prevent a breach. Given the fragmented nature of cybersecurity regulation, utilities may face legal action from the Federal Trade Commission, Securities and Exchange Commission, state attorneys general, the United States Department of Justice, plaintiffs whose data is compromised, and shareholders.[11]

The Federal Trade Commission (FTC) has sued companies for failing to maintain "reasonable and appropriate" cybersecurity protections. In *FTC v. Wynhdam* and *FTC v. LabMD*, the FTC took action against companies under Section 5 of the FTC Act, which grants the FTC authority to investigate "unfair and deceptive practices in or affecting commerce." The cybersecurity policies of Wyndham Hotels and LabMD were determined to be unfair practices causing consumer harm.

State attorneys general have also taken action against companies. Forty-seven states and the District of Columbia require companies or state governments to notify consumers when an unauthorized party accesses their personally identifiable information.[12] Companies such as Accretive Health and the Kaiser Foundation Health Plan have been sued for failing to notify individuals that their information had been compromised.

Business partners sued People's United Bank, Hannaford Brothers, and Heartland Payment Systems when their cybersecurity programs were deemed negligent or commercially unreasonable. Shareholders sued Target and TJX Companies after their cybersecurity breaches. Target's board and senior managers are charged in an ongoing suit with being responsible for the breach and releasing false and misleading statements after the breach, while TJX was charged with breaching its fiduciary duties.

A utility must be aware of the liability obligations it takes on in the cybersecurity realm. Since the states have different laws, there is no one-size-fits-all approach to limiting liability. Utilities may be hesitant to commit to a cybersecurity practice without knowing that the action will satisfy all of the liability requirements that the utility faces. On the federal level, liability protections have been suggested as an incentive for compliance with cybersecurity guidance.[13] However, these protections have yet to be granted, and liability remains a primary concern for utilities.

1.6. Confidentiality

Cybersecurity measures must be implemented with some measure of secrecy. Disclosing exactly how a utility plans to defend against cyber attacks would undermine the effectiveness of those measures, allowing attackers to know exactly what systems and vulnerabilities to be prepared for.[14] As government institutions, many state utility commissions must disclose their

---

[11] Germano & Goldman, 2014

[12] Germano & Goldman, 2014

[13] United States Department of Commerce, 2013

[14] It should be noted that secrecy is not, however, a sufficient security policy. The confidentiality of cybersecurity measures is meant to supplement a greater, developed cybersecurity plan that accounts

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 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.

Confidentiality also complicates the information sharing process, an important piece of current cybersecurity procedures. Since many organizations in both the public and private sectors are involved in combating cybersecurity threats, each of them must be able to communicate with one another about potential threats and responses. Each federal agency involved has different responsibilities, and must share information between governments and private entities. Utilities have to be certain that any information they share with governments or other private companies is treated with the utmost care, and is not used for competitive purposes or divulged to the public. Finally, the existence of critical infrastructure information available only to those with security clearances further complicates information exchange between affected entities and personnel who lack such clearances.

1.7. Technical Knowledge

Commissions may also run into difficulty when they are provided with a utility's cybersecurity information. Commissions may not have the technical knowledge to properly evaluate what a utility is or should be doing to maintain the security of its critical assets. Since it is a commission's responsibility to allow the recovery of prudent expenses, a commission must be able to adequately assess when an expense is or is not prudent. Commissions without an understanding of the components of a comprehensive cybersecurity plan may have difficulty assessing the prudence of claimed expenses.

Traditionally, cybersecurity expenditures have been recovered without special considerations. Utilities have elected to "bake-in" cybersecurity with their normal course of doing business. That is, when a utility purchases a new piece of equipment, they make cybersecurity judgments within that process. Then, the cost of that equipment is recovered through the traditional rate making process. Utilities may not even raise the subject of cybersecurity expenses in a rate case. Consequently, few states have asked cybersecurity questions of their utilities during a ratemaking proceeding.

A cybersecurity breach may not mean that a utility did not make prudent cybersecurity investments, and the lack of a breach may not ensure that such investments were made wisely. Asking utilities to ensure zero breaches would be unreasonable. Cyber vulnerabilities are often discovered well after a system has been developed or implemented and "zero-day" vulnerabilities are completely unknown before an attacker takes advantage of them. Utilities and regulators should expect intrusions to occur. Many cybersecurity experts would argue that every utility has or should expect to be, whether or not the utility is aware of it, breached by cyber

---

for system structure and vulnerabilities.

attacks at some level.[15] Alternatively, a utility without any cyber breaches cannot be assumed to have taken completely prudent action. The utility may have spent money on unnecessary systems or defenses, or be unaware of an intrusion. Here, commissions must be able to properly assess the nuances of claimed cybersecurity expenses. However, reports have indicated that most commissions have little cybersecurity experience, and few have staff members dedicated to this issue.[16]

The challenge of limited technical knowledge is not limited to commissions. Utilities also must possess a strong degree of cybersecurity knowledge. Without proper systems and safeguards in place, utilities may be unaware of intrusions. It is possible for advanced attackers to infiltrate a system without leaving traces, but most breaches will leave behind indications. A utility without the ability to detect intrusions may believe their cybersecurity measures are effective, and forgo fixing their vulnerabilities.

One unsophisticated take on cybersecurity is that of "security through obscurity," the idea that secrecy provides security. According to this theory, attackers will be unable to penetrate a system if they do not know what vulnerabilities it may have. However, the growing capabilities of cyber threats make such an approach unacceptable. "Defense in depth" security -- which includes designing redundant, layered cybersecurity systems[17] -- requires a greater deal of complexity and knowledge, but increases a utility's resiliency against cyber attacks. Developing technical knowledge of cybersecurity is therefore important for all involved in critical infrastructure, but especially to Commissions which are charged with making evaluations of specific plans to protect consumers and utilities.

1.8. New Technologies

Cybersecurity is a fast moving field, with the discovery of specific vulnerabilities and mitigations occurring at a rapid pace. New technologies are also being developed and implemented, each bringing their own risks and appropriate responses. Utilities and regulators must keep up with this tumultuous field through constant vigilance and training.

Cybersecurity threats come from a broad range of technologies. An Advanced Persistent Threat (APT) works with a high level of sophistication to attack vulnerabilities within a specific system and compromise an asset over long periods of time. Spear Phishing targets employees on a personal basis, and encourages individuals to unknowingly compromise their own systems. The growing Bring Your Own Device (BYOD) trend encourages workers to bring their cell phones and laptops into work environments, without necessarily taking the proper steps to ensure the security of those devices. These are just some of the threats that a utility may face, and mitigating each of them requires a utility to be aware of rapid-paced developments. These are

---

15 Ponemon Institute LLC, 2014

16 Behr & Sobczak, 2014, Homeland Security News Wire, 2014

17 Scarfone, Karen et al, 2008

known threats faced today, but expertise to protect and mitigate these threats may not prepare a utility for threats faced in the future.

Accordingly, to best assess the prudence of ongoing cybersecurity measures, understanding that not all businesses will provide the same risk factors, utility commissions must be aware of the changing nature of threats and responses. A utility that developed its cybersecurity program years ago may be unable to defend itself from modern threats. Entirely new technology segments are rapidly introduced and alter how utilities must approach cybersecurity.

The development of new technologies and cybersecurity procedures also makes constructing effective cybersecurity regulations more difficult. While it may be possible for regulators to develop specific and rigid standards for today's cyber-environment, those regulations would quickly be surpassed by changing technologies. Cybersecurity policies require frequent revision, and a utility that merely complied with enacted regulation would become vulnerable to the shifting nature of cyber threats. The time required in creating regulation at the state or federal level is significant enough that best practices may be obviated by technological advances, making the regulation ineffective.

Commission Actions to Date

With the aforementioned responsibilities and challenges in mind, this section will summarize major actions taken by commissions to address cybersecurity. Commissions have adopted new rules and regulations, undergone education and training programs for staff and commissioners, had meetings and briefings with companies, opened case dockets, and undertaken other actions.

However, increased focus on cybersecurity issues has encouraged many state utility commissions to explore the issue. Primarily, commissions have created cybersecurity requirements within their adoption of Advanced Metering Infrastructure (AMI), also referred to as the "smart grid." These requirements usually focus on limiting third-party access to a customer's usage data. Some of these commissions have been given specific instruction from their state legislatures to examine cybersecurity, while others have deemed the subject to be important of their own accord. Few commissions have approached cybersecurity outside of its role in AMI, but those that have required incident reporting, cybersecurity plans, or annual cybersecurity audits. In order to ensure that a utility's cyber response plan is not made available to potential attackers, commissions have made an effort to keep cybersecurity details from becoming public. Some commissions have enacted rules to keep cybersecurity details confidential between the commission and the utility. These actions are needed to balance a commission's responsibility to judge an investment's prudence with the utility's need to protect their cyber response capabilities. Seven state utility commissions have ongoing dockets related to cybersecurity, and further rules may develop from these dockets.

A summary of commission actions on cybersecurity follows. **Table 1** lists the actions taken by commissions, and **Table 2** lists current ongoing dockets examining cybersecurity issues. Those actions and dockets are then further described in Sections 4.1 through 4.5. Section 4.6 details the circumstances in which cybersecurity expenses have been explicitly referenced in

general rate cases. These descriptions are intended to provide other interested commissions with some tools to compare their potential actions with those of their peers. The trends prevalent in commission actions are later summarized and described in Section 6.

Table 1. Commission Actions

Actions Taken		
State	**Docket**	**Description**
Arkansas	10-109-U	Preapproval of AMI costs, required cybersecurity plan
California	11-07-056	Rules for access of private information, annual AMI reports
Connecticut	10-11-08	Cybersecurity questions
Maryland	9207, 9208	AMI deployment plans, annual cybersecurity briefings, cybersecurity auditing firm
Montana	D2013.12.85	Cybersecurity questions
New Jersey	EO11090575	Public safety and reliability, required incident reporting, confidential filing
New York	02-M-0953	Cybersecurity auditing firm, cybersecurity action plan
New York	13-M-0178	Required cybersecurity plan, annual reporting
Oregon	RE 17	Cybersecurity questions
Pennsylvania	52 Pa. Code §§101.1 et seq.	Required cybersecurity plan, annual reporting
Texas	§25.130	Rules for access of private information, annual third party cybersecurity assessments
Washington	U-090222	Annual AMI reports

Table 2. Ongoing Dockets

Ongoing Dockets		
State	**Docket**	**Description**
Connecticut	14-05-12	Standards and oversight procedures
District of Columbia	FC1098	Rules for access of private information
Indiana	44319	Confidential response to commission questions
Kentucky	2012-00428	AMI deployment plans
Louisiana	R-32702	Public safety and reliability, cybersecurity questions
Massachusetts	D.P.U. 12-76	AMI deployment plans
Missouri	EW-2013-0011	Cybersecurity questions
New York	14-M-0101	AMI deployment plans
Rhode Island	4075	AMI deployment plans
South Carolina	2014-416-E	NERC CIP recovery
Vermont	7307	AMI deployment plans, annual cybersecurity briefings

1.9. Rules and Regulations Adopted

1.9.1. Arkansas

By an order issued on August 3, 2011, the Arkansas Public Service Commission (ARPSC) approved a Settlement Agreement and granted pre-approval of Oklahoma Gas and Electric Company's (OG&E) deployment of smart grid technology.[18] The Commission authorized a rider for cost recovery of smart grid costs and directed OG&E to file a comprehensive Customer Information Privacy and CyberSecurity Plan for Commission review and approval, which was granted by the Commission in Order No. 10 on December 15, 2011. That order found that OG&E's filing of its DOE-approved Cyber-Security Plan for the Smart Grid System, Data Privacy Plan, NERC CIP Information Plan, and initial Education Program talking points and proposed budget for Smart Grid in Arkansas satisfied the Commission's earlier directives to provide additional information in support of the Settlement Agreement. The ARPSC further directed OG&E to file a status report in October 2012 detailing

[18] ARPSC Docket No. 10-109-U, Order No. 8

the company's implementation of its information privacy and cybersecurity plan. OG&E's status report was filed in the docket on October 31, 2012.[19]

1.9.2. California

The California Public Utility Commission (CAPUC) developed privacy provisions for AMI data. In Decision 11-07-056, the PUC adopted rules to protect the privacy and security of its utilities' electric usage data. Third parties must receive permission from customers to access data associated with smart meters, and must also notify the commission of cybersecurity breaches. The decision required annual customer information privacy reports from each of the state's electric utilities.[20] The CAPUC is also required to file an annual Smart Grid Report, updating the state's legislature and governor on smart grid advances made by the CAPUC and its regulated utilities. Smart grid deployment plans have been filed by each utility, and include cybersecurity strategies.[21]

1.9.3. Connecticut

The Connecticut Public Utilities Regulatory Authority (CTPURA) conducted a study of its regulated utilities' cybersecurity practices. Through Docket Number 10-11-08, the CTPURA examined the policies of its utilities in order to assess the possibility of enhancements and examine the role of the CTPURA and the state of Connecticut in contributing to more effective cybersecurity plans. The CTPURA asked 65 questions of its utilities, and responses remain confidential or were only available to the CTPURA through on-site visits to the utility.[22]

The CTPURA also released "Cybersecurity and Connecticut's Public Utilities" in April 2014. As directed in Connecticut's Comprehensive Energy Strategy, the CTPURA continued to review the adequacy of its electric, natural gas, and water companies' cybersecurity plans. The report found that Connecticut's utilities had so far enacted adequate cybersecurity protections, and recommended that Connecticut consider annual cyber audits of its utilities, either in the form of self-regulated reports or third-party audits.[23]

1.9.4. Maryland

Maryland has adopted cybersecurity rules under its AMI orders. In Cases 9207 and 9208, the Maryland Public Service Commission (MDPSC) examined the AMI deployment plans of Pepco Holdings Inc. (PHI) and Baltimore Gas and Electric Company (BGE) respectively. The MPSC instructed the PHI companies Potomac Electric Power Company (PEPCO) and Delmarva Power and Light to submit a comprehensive set of metrics for customer privacy and

---

19 Arkansas Public Service Commission, 2011

20 California Public Utilities Commission, 2011

21 California Public Utilities Commission, 2014

22 Wilson, 2012

23 House, 2014

cybersecurity.[24] In a separate proceeding (Case No. 9294), the Southern Maryland Electric Cooperative is in the process of developing its cybersecurity plan in the context of its AMI deployment. BGE joined PHI in a Joint Utility Smart Grid Cyber-Security Process Reporting Plan. A working group between BGE, PHI, the Maryland Energy Administration, Office of People's Council, AARP, and commission staff was unable to reach a full consensus on those metrics, and the utilities proposed actions in lieu of metrics.[25] The MDPSC accepted the utilities' proposal, which included the retention of a cybersecurity consulting firm responsible to the commission and confidential annual briefings. [26]

1.9.5. Montana

The Montana Public Service Commission (MTPSC) asked NorthWestern Energy (NWE) questions about its cybersecurity policies in Docket Number D2013.12.85. NWE was asked to describe how cybersecurity was being maintained, to summarize significant cybersecurity incidents, to address due diligence and known deficiencies in cybersecurity, and to discuss the potential harm from cybersecurity breaches. NWE's responses included confidential material, and both a full response and publically releasable version were provided to the MTPSC.

1.9.6. New Jersey

The New Jersey Board of Public Utilities (NJBPU) instructed all of its regulated utilities to report incidents in which a person accessed an ICS without authorization; unauthorized programs, information, code, or commands were discovered on an ICS; or a person extorted money by threatening to cause damage to an ICS.[27] In Docket Number EO11090575, the BPU interpreted the statutory requirement of utilities to report suspicious activities, including "forced entry to any utility facility, or entry achieved by deception," to include entries or damages to a utility's computer systems. The NJBPU ordered New Jersey's utilities to report past intrusions, and future incidents are to be reported to the NJBPU's Reliability and Security staff within six hours of detection. Additionally, utilities must submit notice of an intrusion to the New Jersey Office of Homeland Security and Preparedness' reporting system, the New Jersey Suspicious Activity Reporting System, within six hours of detection.[28] The order offers utilities the

---

[24] The Public Service Commission of Maryland, 2010

[25] Curry & Micheel, 2012

[26] The Public Service Commission of Maryland, 2013

[27] New Jersey Board of Public Utilities, 2011

[28] See New Jersey Board of Public Utilities, 2011. In Docket EO11090575, the BPU required incident reporting when: "a) A person, including, any individual, firm corporation, educational institution, financial institution, governmental entity, or legal or other entity that accessed your Industrial Control System without authorization or exceeded authorized access. b) Unauthorized programs, information, code, or commands discovered on an Industrial Control System. c) A person extorted any money or other thing of value by threatening to cause damage to your Industrial Control System."

opportunity to submit this information confidentially through the NJBPU's standard confidentiality regulations.

1.9.7. New York

Beginning in 2002, the New York Public Service Commission (NYPSC) expanded its role in overseeing utility reliability to take into consideration the new reality of both cyber and physical malicious threats. In Case Number 02-M-0953, the NYPSC ordered all the major electric, gas, and telecommunications utilities to undergo comprehensive cybersecurity audits by a third-party consultant. Those consultant findings led to a further order by the NYPSC directing each major utility to develop action plans for the implementation of the cyber security improvements identified as needed in the comprehensive audits.

The New York Department of Public Service (NYDPS) required its regulated large energy utilities to prepare new comprehensive cybersecurity plans for energy delivery operations in 2012. In Case Number 13-M-0178, the NYPSC ordered all large electric, gas, and telecommunications utilities to prepare new cybersecurity plans addressing the need for strengthened protection from a cyber-breach of utility customer information, and also calling for annual review at each electric, gas and large water utility of the quality of customer privacy protections by a credentialed third party. Those plans have been evaluated and approved by NYDPS staff and are to be used by the utilities as the basis for ongoing cybersecurity program upgrades.

1.9.8. Pennsylvania

In Docket Number L-00040166, the Pennsylvania Public Utility Commission (PAPUC) adopted rules that require each of its regulated utilities to develop and maintain cybersecurity plans to protect their infrastructure and provide safe, continuous, and reliable service. Utilities must submit an annual self certification form to the PAPUC demonstrating that their cybersecurity plan includes the critical functions requiring automated processing, appropriate backup for application software and data, alternative methods for meeting critical functional responsibilities in the absence of information technology capabilities, and a recognition of the critical time period for each information system before the utility could no longer continue to operate.[29] If a utility must develop a similar plan for another jurisdictional entity, such as the federal government, that plan can meet the PAPUC's requirements. The PAPUC then reviews the utility's self-certification form, and may further review the utility's facilities through the PAPUC's management audit process.

In 2012, the PAPUC developed a work plan of cybersecurity initiatives which included meeting with utilities, state and federal partners, non-jurisdictional entities, and the Commonwealth's Office of Homeland Security to coordinate efforts to communicate and strategize to protect Pennsylvania's utility assets from cyber attacks. In this effort, the PAPUC established an internal multi-disciplinary team of staff including individuals involved in

[29] 52. Pa. Code §101.1 et seq., Act 156 of 2006.

emergency preparedness to coordinate with the utility sector to monitor cybersecurity efforts. In addition, in 2014, the PAPUC finalized a Policy Statement to establish a Critical Infrastructure Interdependency Working Group. Part of the group's mission is for utilities and other affected parties to report and coordinate actions necessary in response to cyber incidents.

The PAPUC continues its work plan currently including PAPUC staff training and additional outreach to its key partners.

1.9.9. Texas

The Public Utility Commission of Texas (PUCT) required independent security audits of its electric utilities deploying AMI in 2007. Rule §25.130 addressed customer and third party access to customer usage data, and called for an initial security audit within a year of implementation. Subsequent PUCT orders instructed certain Texas' utilities to undergo annual third-party cybersecurity assessments as a condition of an AMI surcharge. The PUCT's staff has been involved in selecting the vendor that conducts the assessment, and has reviewed the assessment outcomes.[30]

1.9.10. Washington

The Washington Utilities and Transportation Commission asked its electric utilities to file smart grid technology reports. The reports must describe the smart grid technologies that the utility has considered, and the evaluated details include the cybersecurity of utility operational information and the cybersecurity of customer information. Washington's electric utilities began filing these reports in 2010, and have updated them every other year since.[31]

1.10. Education and Training for Commissioners and Staff

Commissions have recognized that cybersecurity may fall outside of their areas of expertise, and have attended education and training programs. These programs, some of which have been conducted by the National Association of Regulatory Utility Commissioners (NARUC), the Department of Homeland Security (DHS), and the Federal Emergency Management Agency (FEMA), have affirmed the newfound importance and difficulties surrounding cybersecurity.

DHS conducts biennial cybersecurity exercises under its Cyber Storm program. These programs have included the development and evaluation of response plans with officials from 19 states: California, Colorado, Delaware, Idaho, Illinois, Iowa, Maine, Michigan, Minnesota, Mississippi, Missouri, Nevada, New York, North Carolina, Oregon, Pennsylvania, Texas, Virginia, and Washington.[32]

---

30 Rivaldo, 2012

31 Washington Utilities and Transportation Commission, 2010

32 Department of Homeland Security, no date

NARUC offers cybersecurity training programs to its member state utility commissions. Since 2012, the organization has conducted training programs for 37 commissions. These workshops focus on cost recovery, confidential information sharing, and coordination issues. NARUC has also offered grants to state utility commissions that have allowed commissions to examine and explore their role in critical infrastructure cybersecurity.

FEMA has partnered with DHS and Texas A&M University to offer cybersecurity awareness courses for non-technical, IT professional, and business professional audiences. Their non-technical courses include "Information Security for Everyone," and their professional courses include "Cyber Incident Analysis and Response" and "Business Information Continuity." These programs offer online opportunities to examine cybersecurity preparedness.

FERC will review an electric utility's information technology plans to help identify vulnerabilities on a voluntary basis and has allowed states to observe as a training opportunity. For example, PAPUC staff participated in a multi-day architectural review conducted by FERC.

1.11. Company Meetings/Briefings

Commissions and utilities have realized the importance of cooperation in combating cyber threats. To this end, commissions and utilities have had a number of meetings and briefings, so that each is aware of the challenges faced. Commissions have met with their regulated utilities to discuss the threats facing utilities, and the actions utilities have taken to mitigate them. These meetings have occurred both on and off the record, with considerations being granted for the necessary confidentiality surrounding a utility's cyber response plans. As a number of commissions have held confidential meetings with their utilities, the following section is not intended to be inclusive of all commission-utility meetings. Other states that have met with their regulated utilities include Alaska, Indiana, Iowa, Kentucky, Michigan, Oregon, South Carolina, Utah, and Wyoming. This section describes the publicly available meeting details of select meetings, along with meeting descriptions released by those commissions.

1.11.1. District of Columbia

The District of Columbia Public Service Commission (DCPSC) has received cybersecurity briefings from each of its regulated utilities. The briefings are announced at an open meeting where a closed meeting to hold the briefing is then authorized by a vote of the commission. The briefing is held at the utility. The utility retains all documents related to the briefing. These briefings have included a response to questions modeled after the questionnaire in the NARUC Cybersecurity for State Regulators 2.0 as well as the utility's security governance structure and risk mitigation strategies.

1.11.2. Maryland

Maryland has ordered three of its utilities to hold annual cybersecurity briefings with the PSC in conjunction with three AMI dockets: 9207, 9208 and 9294. The meetings are confidential, and the utility retains all documents related to the briefing. The utility may be asked to prepare one copy of the annual report before the meeting, but that report must remain confidential as well. These briefings cover the utility's security framework, security risks,

security protections, security governance structure, security assessments, risk mitigation strategies, changes of additions from the prior report, and a roadmap of cybersecurity items.[33]

1.11.3. New Jersey

In 2013 and 2014, the New Jersey Board of Public Utilities sponsored three Cyber Security Summits in conjunction with the FBI Cyber Crimes Unit, New Jersey Office of Homeland Security and US Department of Homeland Security. These private meetings were attended by cyber security experts from the Electric, Natural Gas and Water sectors in New Jersey. The agendas included FBI and DHS briefings as well as open discussion on cyber security threats, vulnerabilities, utility sector challenges in threat assessment and overlapping jurisdictional concerns.

1.11.4. Ohio

The Public Utilities Commission of Ohio (PUCO) hosted an emergency tabletop exercise with representatives from utility industry stakeholders in 2011. The exercise, which included staged responses to a variety of reliability threats, included presentations on improving energy sector cybersecurity by the Department of Energy, Department of Homeland Security, Federal Bureau of Investigation, and Ohio Department of Public Safety representatives. PUCO has continued to hold meetings with electric, gas, and water utilities through the Ohio Critical Infrastructure Collaborative.

1.11.5. Pennsylvania

The PAPUC continues to be actively engaged in the issue of cybersecurity in continuing its collaboration over the last two years with the US Department of Homeland Security, the PA Office of Homeland Security and other federal and state partners. The PAPUC was instrumental in establishing a Middle Atlantic Cybersecurity Collaborative among six states including New Jersey, Pennsylvania, Delaware, Maryland, Washington, D. C and Ohio to provide opportunities for education and communications sharing in light of the reality that cyber incidents can affect several regions.

The PAPUC has convened stakeholder meetings with utilities and non-jurisdictional critical infrastructure owners to share best practices and information about security threats. The Commission has also partnered with the US DHS to provide training to industry representatives on cybersecurity planning. In addition, the PAPUC participates in an intra-agency work group focused on critical infrastructure cybersecurity planning and response.

The PAPUC also hosted a Commission wide cyber training session presented by the Chief Information Officer for the Commonwealth. This session provided additional information to all employees in attendance so that they better understood current cyber threats to both the Commonwealth's network and the regulated communities.

---

[33] The Public Service Commission of Maryland, 2013

1.11.6. South Carolina

The South Carolina Public Service Commission (SCPSC) held a briefing with Duke Energy Progress to discuss smart meters in September 2014. During proceeding #14-11441, the SCPSC's commissioners asked Duke's representatives about how third parties could access smart meter data, the utility's compliance with NIST standards, and privacy concerns associated with smart meters.

1.11.7. Texas

PUCT has been involved in a number of industry and standards groups. The PUCT has monitored the development of standards and attends stakeholder groups, including the Electric Reliability Council of Texas Critical Infrastructure Protection Working Group, as part of its ongoing physical and cybersecurity project. In developing its AMI rule, commission staff had multiple informal meetings with its utilities to examine their cybersecurity practices, and continues to informally communicate with utilities on the importance of grid security.[34]

1.12. Ongoing Case Dockets

1.12.1. Connecticut

The CTPURA opened Docket Number 14-05-12 in May 2014 to address the questions raised within its "Cybersecurity and Connecticut's Public Utilities" report. The docket intends to "produce a set of compliance standards and oversight procedures to strengthen the State's cybersecurity defense capabilities." CTPURA has begun the process of hiring a consultant with experience in cybersecurity and building defense mechanisms to assist in completing the docket.

1.12.2. District of Columbia

In response to a petition by a third party supplier, DCPSC opened an investigation regarding third-party supplier access to PEPCO's smart meter data. As part of that docket, FC1098, the DCPSC asked its third-party suppliers to provide the commission with a copy of their written cybersecurity policies or a description of how the company addresses cybersecurity concerns.[35]

1.12.3. Indiana

The Indiana Utility Regulatory Commission (INURC) has made cybersecurity information requests to its jurisdictional utilities. The commission found that its utilities are "required to furnish reasonably adequate service and facilities," and that the commission is "authorized to conduct investigations into a utility's provision of service and to request

---

[34] Rivaldo, 2012

[35] Public Service Commission of the District of Columbia, 2014

information from utilities required to fulfill the Commission's statutory obligations."[36] The commission therefore opened a docket for its utilities to respond to their cybersecurity questions confidentially. The utilities' responses are confidential because they have a "reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack if publicly disclosed," in accordance with Indiana's Access to Public Records Act.[37]

1.12.4. Kentucky

Kentucky's Public Service Commission (KYPSC) has opened Case Number 2012-00428: Consideration of the Implementation of Smart Grid and Smart Meter Technologies. The KYPSC has asked all of its electric utilities to "describe the precautions taken and/or standards developed by the utility to address concerns regarding cybersecurity and privacy issues," and both its electric and gas utilities to describe cybersecurity policies or identify industry or national standards for cybersecurity.[38] The KYPSC held multiple informal conferences with its utilities to discuss smart grid standards, and has granted its utilities the ability to file their cybersecurity policies confidentially.[39]

1.12.5. Louisiana

The Louisiana Public Service Commission (LAPSC) opened Docket No. R-32702 in February 2013. The Docket calls for the study and possible implementation of rules regarding the cybersecurity of utility computer systems. Commission staff was directed to address the actions the LAPSC can take to ensure public safety and reliability, how the NERC-CIP standards can be applied to the distribution grid, what regulatory mechanisms can be implemented to ensure cybersecurity, how the LAPSC can ensure proper incentives to address cybersecurity, what requirements the commission should develop to ensure resiliency, what metrics are needed to track the effectiveness of cybersecurity policy and investments, and how confidentiality rules apply to cybersecurity.[40] The commission expects to present its policy recommendations in September 2014.[41]

1.12.6. Massachusetts

The Massachusetts Department of Public Utilities (MADPU) began investigating the modernization of its electric grid in October 2012. The MADPU's "modern grid" is similar to other states' efforts to develop smart grid technologies. One area of inquiry identified in the MADPU's order opening the investigation was that of Health, Interoperability, Cybersecurity,

---

36 Indiana Utility Regulatory Commission, 2013

37 Indiana Utility Regulatory Commission, 2013

38 Kentucky Public Service Commission, 2013

39 Kentucky Public Service Commission, 2014

40 Louisiana Public Service Commission, 2013

41 Louisiana Public Service Commission, 2014

and Privacy. The MADPU asked: "What steps should the Department take to address cybersecurity and privacy concerns associated with grid modernization?"[42] The MADPU instructed its electric utilities to file 10-year Grid Modernization Plans, including descriptions of each company's strategies for ensuring cybersecurity. In the meantime, the MADPU is examining available voluntary cybersecurity standards and frameworks, and their applicability to the overall operations of electric and gas distribution companies.[43]

1.12.7. Missouri

Missouri has opened a working docket on effective cybersecurity practices. The Missouri Public Service Commission (MOPSC)'s docket EW-2013-0011 is an ongoing effort to explore the integrity of its utilities' cybersecurity practices. The MPSC found that "because cybersecurity threats challenge the reliability, resiliency and safety of the grid, and because utility spending to address cyber vulnerabilities can impact the bills that customers pay, the Commission must explore, and ensure, the integrity of the electric utilities' internal cybersecurity practices."[44] The commission asked its utilities 47 questions, focusing on planning, standards, procurement practices, personnel and policies, and systems and operations. These questions are modeled after NARUC's sample questions presented in *Cybersecurity for State Regulators 2.0*.[45] The MOPSC's staff filed a confidential report summarizing their utilities' responses to the questions and making specific recommendations in February 2013. In March 2013, the MOPSC issued an order directing stakeholders to conduct further discussions and formulate an informal reporting schedule, wherein the electric utilities are required to orally provide information to designated members of the MOPSC staff.

1.12.8. New York

The NYPSC has begun a review of the state's regulatory structure. The NYPSC "announced that we will comprehensively consider how our regulatory paradigm and retail and wholesale market designs either effectuate or impeded progress toward achieving the policy objectives underlying our system benefit programs and our regulation of electric distribution utilities."[46] The commission's staff created a report detailing the policy objectives within their vision for the state's energy future, and identified cybersecurity questions that must be answered. These questions ask what communications networks are needed to support the integrated grid and how utilities will protect cybersecurity of the integrated distribution system. As a result, a Platform Technology Working Group examined the standards and protocols relevant to cybersecurity, and found no acceptance of common cybersecurity schemes across its utilities.

---

42 Massachusetts Department of Public Utilities, 2012

43 Massachusetts Department of Public Utilities, 2013

44 The Public Service Commission of the State of Missouri, 2012

45 Keogh & Cody, 2013

46 State of New York Public Service Commission, 2014

The Working Group's Technologies Subgroup recommended that, moving forward, "cyber-security must take precedence in platform implementation."[47]

1.12.9. Ohio

PUCO currently has a pending Electric Security Plan case with American Electric Power (AEP) wherein AEP has requested recovery for NERC CIP expenses. First Energy has also requested a broad rider designed to pick up security costs. These cases are ongoing, and PUCO has yet to assess the requests.

1.12.10. South Carolina

In October 2014, South Carolina Electric & Gas Company (SCE&G) petitioned the SCPSC seeking authorization to defer $20 million for depreciation and amortization expenses and incremental operation and maintenance expenses associated with NERC CIP compliance during the five-year period of 2015 to 2019. SCE&G estimated that complying with the CIP standards would require $41 million of infrastructure upgrades. The associated annual increase in depreciation and amortization expense will be $800,000, and the annual increase in operations and maintenance will be $3.3 million. SCE&G asked the commission to defer these costs as a regulatory asset until rate recovery could be approved in SCE&G's base rates. Docket Number 2014-416-E remains open.

1.12.11. Vermont

The Vermont Public Service Board (VTPSB) opened Docket 7307: Smart Metering and Alternative Rate Design in 2007. The docket includes a memorandum of understanding between the VTPSB and the Vermont Department of Public Service (VTDPS) detailing a six-part cybersecurity proposal that would require utilities deploying smart grid programs to create a smart grid cybersecurity plan. The utilities would meet with the VTDPS twice annually to discuss updates or amendments to the plan, the impact of new state or federal cybersecurity standards, and areas of prospective collaboration between the utilities and the VTDPS. The VTDPS and utilities would then offer an annual report to the VTPSB that includes a list of all known attacks or attempts, the outcomes and steps taken to address those attacks or attempts, and a plan for future action. Utilities would be required to, in the event of an attack or system compromise, comply with reporting standards and take steps to mitigate future breaches.

1.13. Other Actions

1.13.1. District of Columbia

The DCPSC modified its discovery rules for formal proceedings to include a new confidential discovery procedure that applies to requests for critical infrastructure information.[48]

---

[47] Technologies Subgroup, 2014

[48] 15 DCMR §15-151

The DCPSC also requested that its legislative body enact a new exemption under the District of Columbia Freedom of Information Act for "critical infrastructure information." Temporary legislation was passed, and permanent legislation is pending.

1.13.2. Maryland

The MDPSC required its electric utilities to create a public fact sheet on cybersecurity policies in order to supplement confidential meetings. As a requirement of the utilities' AMI deployment, BGE, PEPCO, and Delmarva have provided "basic publicly available information on how the Utility is protecting its AMI and the responsible Utilities' organization for cyber-security."[49] The companies have further filed reports addressing cybersecurity topics including a project overview, an introduction to cybersecurity, the utility's framework for ensuring cybersecurity, the governing process responsible for ensuring cybersecurity, an overview of the risk assessment process, the architecture and design of cybersecurity, and a review of key topics of the report.[50]

1.13.3. New York

In 2003, the NYPSC approved the creation and staffing of a new Utility Security Section within the NYDPS. The section is responsible for monitoring the performance of the utility companies in strengthening their cyber and physical security preparedness on an ongoing basis. Since then, NYDPS Utility Security staff have conducted regular on-site evaluations of the cybersecurity measures, practices, and procedures at each utility to ensure that critical digital control systems are well protected against malicious external and internal attacks and other forms of potential cyber systems disruption.

1.14. Direct Consideration Within Rate Cases

1.14.1. Florida

The Florida Public Service Commission (FLPSC) has considered cybersecurity expenses within multiple rate cases. The FLPSC approved incremental O&M security and NERC cybersecurity expenses for Tampa Electric Company (TECO) in Docket Number 080317-EI. In Docket Number 110001-EI, TECO proposed the additional recovery of incremental cybersecurity costs totaling $295,465 during 2012. TECO testified that it expected to incur incremental costs associated with future NERC CIP requirements in 2013 and 2014. However, TECO withdrew the proposed charge in a later stipulation.

Gulf Power Company identified $585,000 of NERC CIP compliance and cybersecurity measures in Docket Number 130140-EI. These costs were included within the utility's production capital additions budget, and were split across 2013 and 2014. NERC CIP compliance was the most costly aspect of the utility's expenditure, totaling $413,000 in 2013. An

---

[49] Curry & Micheel, 2012

[50] Curry & Micheel, 2012

additional $86,000 was budgeted annually for cybersecurity measures. Gulf Power also detailed the specific plants that these expenses were associated with, splitting the cost between its Daniel and Smith plants.

The Florida Public Utilities Company (FPU) identified an increase in corporate costs in Docket Number 140025-EI. The increases from FPU's test year totaled $384,268, and included costs associated with enhancing the utility's cybersecurity. The Florida Office of Public Counsel (FLOPC) contested the increase in corporate cost, and a representative of Chesapeake Utilities Corporation (CUC) testified that they had hired external consultants to examine their cybersecurity practices, and planned to hire an in-house cybersecurity manager. The FLOPC continued to protest the increase, but did not object to the cybersecurity expenses. The docket concluded with a settlement.

1.14.2. Idaho

In direct testimony before the Idaho Public Utilities Commission, representatives of Avista Corporation, an electric and natural gas utility, cited cybersecurity expenditures during general rate cases. In Case Numbers AVU-E-10-01 and AVU-G-10-01, Avista added two cybersecurity positions to "focus on meeting new network security compliance requirements from NERC," and also filed for other security and compliance support expenditures. Avista also referenced cybersecurity expenditures in Case Numbers AVU-E-12-08 and AVU-G-12-07. The utility noted that operations and maintenance costs had increased, partially due to cybersecurity expenditures. Each of these cases ended with a settlement, and no further discussion of cybersecurity expenses.

1.14.3. Illinois

In Docket Number 13-0301, the Illinois Commerce Commission (ILCC) set a revenue requirement for Ameren Illinois Company (AIC) authorizing the recovery of $19.9 million and $16.2 million for plant additions in 2012 and 2013, respectively. These plant additions were associated with Illinois' Energy Infrastructure Modernization Act, which required Illinois' utilities to invest in system upgrades and modernization projects. ILCC staff identified and categorized the expenses included within this total, which included $600,000 and $2.2 million for an "associated cyber secure data communications network" in 2012 and 2013. AIC agreed to the categorization, and the ILCC approved recovery of these costs.

1.14.4. Oregon

The Oregon Public Utility Commission (ORPUC) is reviewing an ongoing rate case with Avista Utilities, Docket Number 14-07-G. In Avista's initial filing, the utility identified cybersecurity costs within their enterprise security and information technology expenses. Enterprise security was estimated to cost $286,000 and $49,000 in 2014 and 2015 respectively. Avista noted that cybersecurity and regulatory requirements, particularly those associated with NERC CIP and Executive Order 13636, are two of the primary drivers of this cost. Increasing cybersecurity requirements also were identified as a driver of increased information systems expenses.

1.14.5. Rhode Island

In 2009, National Grid requested recovery for costs associated with NERC CIP requirements from the Rhode Island Public Utilities Commission (RIPUC). In Docket Number 4065, the utility responded to a data request from the Rhode Island Division of Public Utilities and Carriers (Division) that asked for a detailed breakdown of the utility's capital investments in 2009 and 2010. The utility indicated that it had spent $104,900 on "preliminary work for NERC-CIP requirements" and "work for NERC CIP Cyber Security." National Grid also estimated that they would spend a further $21,500 for preliminary work in 2010. The RIPUC included these costs within the utility's forecasted capital additions in its decision.

1.14.6. South Carolina

In Docket Number 2013-59-E, Duke Energy Carolinas proposed a $220 million revenue increase. Within that rate case, Duke noted an increase in the operations and maintenance (O&M) cost associated with its nuclear fleet due to compliance with NRC cybersecurity requirements. The O&M increase also included other factors, such as compliance with new regulations adopted in light of the Fukushima incident. Cybersecurity expenses were not enumerated, and the rate case ended in a settlement that increased revenue by roughly $118.6 million.

1.14.7. South Dakota

In Docket Number EL11-019, Xcel Energy identified cybersecurity costs as a piece of their regulatory compliance requirements. These costs also included items such as fitness for duty standards, physical security rules, and fire protection and emergency preparedness requirements imposed by the NRC and NERC. In Docket Number EL12-061, Black Hills Power, Inc. also noted that NERC CIP requirements had caused its regulatory compliance costs to increase. Each of these dockets concluded with a settlement, and without further mention of cybersecurity expenses.

Docket Number EL140-058 contains significant discussion of Xcel Energy's cybersecurity plans and expenses. In this ongoing docket, Xcel has asked the South Dakota Public Utilities Commission (SDPUC) to approve capital additions totaling $12.7 million for a nuclear plant cybersecurity project. The cost was broken down into contract services, materials, labor, utility/other, and allowance for funds used during construction (AFUDC).[51] Xcel developed the plan in response to regulations published in 2009 by the NRC, and implementation began in 2014.

Actions Taken by Other Entities

State utility commissions are not the only entities interested in cybersecurity. The importance of utilities to the United States' security and economy has led federal agencies, state

[51] The amount attributed to each of these categories is confidential and unavailable to the public.

legislatures, and utility organizations to address utility cybersecurity. Some of these actions have been required by law, while others take the form of voluntary guidelines.

The distinction between mandated requirements and voluntary guidelines is important in cybersecurity. There is a great deal of interest in regulating cybersecurity standards for Critical Infrastructure sectors, which include the communications, energy, and water and wastewater sectors.[52] Protecting privately owned critical infrastructure from advanced persistent threats, including foreign criminals and governments, is an important task, yet it is unreasonable to expect all private utilities to have the resources available to combat such an advanced adversary. However, the federal government has expressed a hesitance to create strict regulations.

This has led to a reliance on public-private partnerships, and a large number of involved actors. The executive branch has instructed a large variety of agencies to focus on cybersecurity issues across sectors. Since cybersecurity is an issue that impacts businesses beyond the utility industry, pieces of the cybersecurity puzzle are broadly dispersed across the federal government.

State legislatures have also addressed cybersecurity. Some states have tended to focus on the role of cybersecurity in relation to development of the smart grid. Other states have taken an all hazards approach to emergency preparedness including all utilities and cybersecurity. States have also created cybersecurity coordinator positions within their governments to facilitate communication between state, federal, and private interests. Beyond that, state legislatures are also concerned with the economic impact of bringing cybersecurity research to their states.

In the spirit of public-private partnerships, utility organizations have made efforts to create private, voluntary standards. While most federal standards are meant to apply across multiple industries, these standards offer sector-specific cybersecurity advice.

1.15. Federal Agencies

A number of federal agencies have expressed responsibility for at least some piece of cybersecurity. While over 50 federal laws address the issue of cybersecurity, there is no singularly responsible agency or piece of legislation. The last major cybersecurity legislation was passed in 2002, when the Homeland Security Act and the Cyber Research and Development Act granted cybersecurity responsibilities to the Department of Homeland Security and National Institute of Standards and Technologies. Without clear guidance from Congress, the executive branch has led the development of federal cybersecurity regulation. The Department of Homeland Security holds the responsibility to coordinate between each of the relevant federal agencies. These agencies include:

- The Department of Commerce;

---

[52] The Department of Homeland Security defines the Critical Infrastructure sectors as the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems sectors.

- The Treasury Department;
- The Environmental Protection Agency;
- The Department of Transportation;
- The Department of Justice;
- The Federal Emergency Management Agency;
- The Federal Communications Commission;
- The Department of Health and Human Services;
- The Department of Energy;
- The Central Intelligence Agency;
- The Department of State;
- And the Department of Defense.

These agencies have worked together to create a voluntary framework for cybersecurity governance. Efforts have been made in recent years to improve federal cybersecurity regulation by allowing for greater information sharing, extending liability protections, and improving cybersecurity research and development. Despite being introduced in multiple sessions of Congress, these reforms have not been passed. Three presidents – Clinton, Bush, and Obama – have worked to address these deficiencies through executive action.

1.15.1. President Clinton

President Clinton established the Commission on Critical Infrastructure Protection, which studied vulnerabilities and protection strategies for critical infrastructure. The commission's report in 1997 recommended the pursuit of a public-private partnership approach towards cybersecurity.[53] Subsequently, Presidential Decision Directive 63 (PDD-63) established a number of new organizations with the intent of protecting the nation's critical infrastructure from cyber attacks. They included the National Infrastructure Protection Center and the Information Sharing and Analysis Centers (ISACs) for each of the critical infrastructure sectors. PDD-63 split cybersecurity responsibility by sector, with eleven agencies coordinating through a newly created National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. Agencies given responsibility relevant to that of state utility commissions include the Environmental Protection Agency, Department of Transportation, Department of Commerce, and Department of Energy.

1.15.2. President Bush

President George W. Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. These directives focused on improving cybersecurity practices of the federal government by creating the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI instructed DHS to examine suggested policy and resource requirements for critical infrastructure and made attempts to improve coordination between the agencies given cybersecurity responsibilities under PPD-63.

---

[53] President's Commission on Critical Infrastructure Protection, 1997

The Director of National Intelligence (DNI) was asked to connect a number of cyber centers into the newly created National Cybersecurity Center (NCC). The NCC was tasked with developing a comprehensive approach to cybersecurity and anticipating future threats.

1.15.3. President Obama

President Obama built on the work of the CNCI following his "Cyberspace Policy Review." The report noted that the federal government could not abdicate its role in cybersecurity, but also that the private sector ownership of critical infrastructure remained important to respect. It emphasized information sharing, a framework for incident response, and called for incentive mechanisms to promote improved security. Pursuant to another recommendation, President Obama created the position of White House Cybersecurity Coordinator, who would be responsible for cybersecurity coordination across federal agencies. President Obama followed these actions with Executive Order 13636 (EO 13636) and Presidential Policy Directive 21 (PPD-21). EO 13636, Improving Critical Infrastructure Cybersecurity, focuses on information sharing and the protection and identification of high priority critical infrastructure. The order expanded DHS' Enhanced Cybersecurity Services (ECS) program to serve all critical infrastructure sectors[54] and instructed the National Institute of Standards and Technologies (NIST) to begin the process of developing a cybersecurity framework for usage across all critical infrastructure sectors. PPD-21 sought to:

- clarify the relationship between the interacting federal agencies;
- improve information sharing and incident response programs; and,
- promote cybersecurity research and development efforts.

1.15.4. Department of Homeland Security

The Department of Homeland Security (DHS) was granted responsibility for many aspects of cybersecurity upon its creation in 2002. DHS is responsible for providing threat and vulnerability information, crisis-management support, and technical assistance for recovery plans to state governments and private companies. The Homeland Security Act (HSA) of 2002 included the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, which allows DHS to grant liability protection for designated technologies used in response to an act of terrorism. The HSA also created methods for DHS to share information among federal agencies, state and local governments, and critical infrastructure personnel.

DHS operates a number of cybersecurity-focused branches. The National Cybersecurity and Communications Integration Center (NCCIC) monitors cyber threats and shares information with private industry through sector-specific branches, including the United States Computer Emergency Readiness Team (US-CERT) and the critical-infrastructure-specific Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). US-CERT seeks to "improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation." The ICS-CERT offers greater response capabilities to critical infrastructure systems. This includes more tangible benefits to critical infrastructure

---

[54] Previously, ECS was only available to members of the defense industry.

organizations, such as incident response and mitigation strategies. ICS-CERT and US-CERT work together within DHS to provide support to critical infrastructure stakeholders.

DHS is largely responsible for leading coordination between the many federal agencies with cybersecurity responsibilities. The National Cybersecurity Center connects the National Cyber Investigative Joint Task Force, National Security Agency/Central Security Service Threat Operations Center (NTOC), Joint Task Force-Global Network Operations, Defense Cyber Crime Center, US-CERT, and the Intelligence Community Incident Response Center. DHS operates the Critical Infrastructure Partnership Advisory Council (CIPAC). CIPAC includes sector-specific councils for each critical infrastructure sector, including the Energy Sector;[55] Nuclear Reactors, Material, and Waste Sector; and the Water and Wastewater Systems Sector. These committees include a mix of federal, state, and private sector representatives.

DHS also conducts cyber event response exercises under the Cyber Storm program. Cyber Storm is a biennial program mandated by Congress to assess cyber preparedness in the public and private sectors. The program has interacted with State governments to examine the roles of all involved in a response to a cyber incident.

1.15.5. Transportation Security Administration

Within DHS, the Transportation Security Administration has regulatory oversight of the security of natural gas and oil pipelines. The TSA's Pipeline Security Division oversees the agency's pipeline cybersecurity programs. The TSA relies on voluntary compliance with its best practice recommendations, including cybersecurity recommendations. Their *TSA Pipeline Security Guidelines* notes, in the spirit of voluntary guidelines, "nothing in this document shall supersede Federal regulatory requirements. This document is guidance. It does not impose mandatory requirements on any person. The term 'should' means that the TSA recommends the actions described."[56] Natural gas trade groups such as the Interstate Natural Gas Association of America have expressed their support for the TSA's cybersecurity measures.[57]

All pipeline cyber assets should, according to the TSA, have baseline cybersecurity measures, including general cybersecurity measures; information security coordination and responsibilities; system lifecycle considerations; system restoration and recovery plans; intrusion detection and response, trainings; and access control and functional segregation. The TSA recommends that pipeline operators identify cyber assets essential to safety and reliability as critical, requiring enhanced security measures. These enhanced measures include further access controls and periodic vulnerability assessments.[58]

---

[55] The Energy Sector Committee is further divided into the Electricity Sub-Sector and Oil and Natural Gas Sub-Sector.

[56] Transportation Security Administration, 2011

[57] Santa, 2012

[58] Transportation Security Administration, 2011

The TSA also recommends a number of planning and implementation documents, including reports by the American Chemistry Council, American Gas Association, American National Standards Institute, American Petroleum Institute, the National Institute of Standards and Technology, and DHS. Further, the TSA recommends that pipeline operators consult cybersecurity references frequently in order to develop and review their security policies in light of technological changes.

1.15.6. Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) regulates the interstate transmission of energy products, such as electricity, natural gas, and oil. Among their responsibilities, FERC is tasked with ensuring the reliability of interstate electricity transmission lines. FERC has therefore created reliability standards, including those for cybersecurity. Together with the North American Electric Reliability Corporation (NERC), FERC has required that bulk electric suppliers comply with its Critical Infrastructure Protection (CIP) standards.

The North American Electric Reliability Corporation (NERC) has been tasked with developing cybersecurity rules for critical infrastructure. Utility companies with assets whose disruption would impact the bulk electric system's reliability must comply with these requirements. NERC's CIP standards, most recently updated to Version 5, instruct those utilities to classify their cyber systems as High, Medium, or Low Impact, and apply a number of requirements to each of those classifications. The CIP Standards are notably one of the few enforceable cybersecurity requirements.

NERC's standards will continue to develop as cyber threats and responses continue to develop. The standards are an evolving document, with four revisions occurring since version one's inception in 2007. Utilities subject to the CIP Standards must remain informed of each revision's changes, and adjust their policies appropriately. NERC's CIP Standards require employee training, physical security measures, and detailed incident response plans, among other requirements. Additionally, NERC is developing requirements for transient electronic devices, such as flash drives and laptop computers.

NERC has conducted grid security exercises through its GridEx program. The exercises, conducted in 2011 and 2013, simulated coordinated cyber and physical attacks on the bulk electric system, and featured representatives from NERC, industry, and government agencies. Each exercise led to a summary report, which recommended improvements for both industry and NERC itself, and NERC will continue the program with GridEx III in 2015.[59]

NERC also operates the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The ES-ISAC coordinates information sharing between utilities, the federal government, and other critical infrastructure sectors. The ES-ISAC offers utilities the opportunity to share cybersecurity experiences and response methods, while allowing a utility to gain information

[59] North American Electric Reliability Corporation, 2012a and North American Electric Reliability Corporation, 2014.

about vulnerabilities and threats. It coordinates with DHS through the National Cybersecurity and Integration Center. Participation in the ES-ISAC is, unlike compliance with the CIP Standards, voluntary. Finally, NERC operates the Electricity Sub-Sector Coordinating Council (ESCC). ESCC has responsibility for developing sector-wide policy initiatives to improve grid reliability through physical and cybersecurity.[60]

1.15.7. Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) is responsible for the safety regulation of private-sector usage of nuclear materials.[61] Under NRC's regulations, all nuclear utilities must have a cybersecurity program. NRC issued specific requirements for certain cyber threats and vulnerabilities after September 11, 2001, and their requirements have continually developed since then. NRC has produced self-assessment tools for nuclear power plants, and endorsed programs intended to help nuclear plants establish and maintain cybersecurity programs.

Nuclear power plants must submit a cybersecurity plan and implementation timeline to NRC for approval, and NRC has published a guide of best practices for compliance. The guide, *Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities*, offers nuclear utilities best practices for assuring the protection of their cyber assets.[62] Utilities must protect systems and networks associated with safety-relayed functions, security functions, emergency preparedness, and support systems and equipment important to safety and security.[63] Nuclear power producers must submit a plan covering these protections, and NRC then enforces the implementation of that plan.

1.15.8. National Institute of Standards and Technology

Among the priorities for cybersecurity regulation has been the promotion of cybersecurity research and development training and studies. The National Institute of Standards and Technology (NIST) and the National Science Foundation (NSF) have been the primary organizations tasked with expanding cybersecurity research. The Cyber Security Research and Development Act of 2002 instructed NSF to award grants for cybersecurity education programs at the undergraduate and graduate levels, while also creating centers for cybersecurity research. NSF accounts for the largest non-defense cybersecurity R&D spending.[64] Pursuant to the Cyber Security Research and Development Act, NIST also awards postdoctoral and senior research fellowships in cybersecurity, and assists in cybersecurity research.[65]

---

60 North American Electric Reliability Corporation, 2012b

61 United States Nuclear Regulatory Commission, 2013

62 United States Nuclear Regulatory Commission, 2010

63 United States Nuclear Regulatory Commission, 2010

64 Fischer, 2013

65 Fischer, 2013

NIST has been tasked with developing a cybersecurity framework, intended to be applicable across critical infrastructure industries. Under EO 13636, NIST released its *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014. The framework focuses on the business case for cybersecurity, and applies organizational "Profiles" to recommend cybersecurity activities based on business requirements, risk tolerances, and resources. NIST emphasizes the voluntary nature of the framework, but contends that it offers organizations the ability to apply principles and best practices of risk management.[66] This framework is subject to continual development, and NIST has announced an extensive roadmap of next steps, including considering the transition of the framework to a private organization with the capability to improve procedures across the framework.[67]

NIST has also published a number of technical documents detailing cybersecurity procedures, such as introductory level guides, smart grid security best practices, and technical explanations of ICS security. These documents are aimed at providing private entities with actionable best practices and technically detailed descriptions of secure procedures.

1.15.9. Federal Communications Commission

The Federal Communications Commission (FCC) enforces Customer Proprietary Network Information (CPNI) rules. The CPNI rules allow telecommunications companies to use CPNI data for specific purposes, including billing initiating new service, and repairing service problems. CPNI data includes billing data, service installation data, account information, and other individually identifiable data.[68] Customer data can be shared in the aggregate, as a raw subscriber list, or when needed for law enforcement purposes with a subpoena. The FCC requires companies to educate employees regarding the uses of private data. Also, telecommunications companies must develop written information protection policies and customer notification mechanisms to be implemented in an instance where data protection methods did not work properly.[69]

The FCC has adopted, and is in the process of updating, a series of best practices for the telecommunications industry through the Communications Security Reliability Interoperability Council (CSRIC). CSRIC is a public private partnership of federal agencies, state utility commissioners, and the telecommunications industry. CSRIC has provided recommendations to ensure the optimal security and reliability of communications systems, which included encouraging information sharing and continued review of cybersecurity practices.[70]

---

66 National Institute of Standards and Technology, 2014

67 National Institute of Standards and Technology, no date

68 Lichtenberg, 2010

69 *FCC-02-214, §64-2009(f)*

70 Communications Security, Reliability, and Interoperability Council, 2013

1.16. State Legislatures

State legislatures have passed relatively little cybersecurity regulation. States have created positions to coordinate cybersecurity activities between state governments, the federal government, and private interests. A number of states have viewed cybersecurity through an economic lens, sensing the opportunity to create jobs and revenue. Few state legislatures have directed their utility commission to examine cybersecurity. The legislatures that have focused on AMI development and the role of cybersecurity in protecting ratepayers' personal information.

The legislatures of California, Illinois, Maine, Oklahoma, Pennsylvania, and Vermont have passed bills that advance AMI development within their state while keeping cybersecurity in mind. The bills limit how utilities can use customer data, create requirements for the storage of that data, or encourage utility investment in cybersecurity. Florida, Hawaii, Maryland, Ohio, and Texas have created councils that examine how the cybersecurity industry can offer their state economic opportunities. Finally, Hawaii, Maryland, and Texas have designated officials or committees with authority for monitoring national cybersecurity standards and facilitating communication between their private entities and other federal or state agencies with cybersecurity responsibilities.

1.16.1. California

The CAPUC was tasked with developing a smart grid deployment plan.[71] The state legislature included in its definition of a smart grid "cost-effective full cyber security," instructing the PUC to include measures for cybersecurity within its smart grid deployment plan. Under Senate Bill 17 of 2009, the PUC must annually file a report to the governor detailing the state's Smart Grid advances. California also enacted protections of customer usage data gathered through AMI. Californian utilities must "use reasonable security procedures and practices to protect a customer's unencrypted electrical consumption data from unauthorized access, destruction, use, modification, or disclosure…"[72] Utilities can share usage data only when that data has been stripped of identifying information.

1.16.2. Colorado

Colorado created the Colorado Smart Grid Task Force in 2012.[73] The task force examined cybersecurity issues, ultimately recommending that NIST standards be respected. Its report recommended that smart grid deployment include relevant standards from additional critical infrastructure sectors.[74] The Smart Grid Task Force will disband July 1, 2015.

---

71 State of California, 2012

72 State of California, 2012

73 State of Colorado, 2012

74 Colorado Smart Grid Task Force, no date

1.16.3. Florida

Florida created a Cybercrime Office within its Department of Law Enforcement in 2011. The Cybercrime Office investigates violations of state laws pertaining to information technology and assists in incident response and recovery, among other responsibilities.

As of July 2014, Florida has also established the Florida Center for Cybersecurity. The Center was tasked by the Florida legislature with developing a cybersecurity education program and interacting with state businesses and military installations. Located at the University of South Florida, the program will begin fall 2014.

1.16.4. Hawaii

In 2014, Hawaii created a cybersecurity, economic education, and infrastructure security coordinator within the state's Department of Defense. The coordinator is to oversee cybersecurity and cyber resiliency within Hawaii, and interacts with State agencies, federal agencies, and public utilities. The coordinator is tasked with (a) improving cyber resiliency for Hawaii's critical infrastructure and State resources; (b) facilitating the growth of Hawaii's cybersecurity industry; and (c) promoting information sharing amongst those threatened by cybersecurity attacks.

1.16.5. Illinois

Illinois created an infrastructure investment program, seeking voluntary utility participation. Participating utilities were instructed to invest in a number of areas, including smart grid cybersecurity. Illinois' smart grid definition includes "dynamic optimization of grid operations and resources, with full cyber security."[75] Commonwealth Edison and Ameren Illinois participate in the program, and have filed plans with the Illinois Commerce Commission since the program's inception.[76]

1.16.6. Maine

Maine adopted a declaration of policy on smart grid infrastructure in 2010.[77] The legislature, seeking to improve reliability and reduce ratepayer cost, energy consumption, and greenhouse gas emissions, acted to promote the development and implementation of AMI technologies. The act gave Maine's Public Utilities Commission the ability to adopt rules on cybersecurity and protection of consumer privacy.

Maine's legislature followed this action with 2011's Resolve to Examine Cyber Security and Privacy Issues Relating to Smart Meters.[78] The PUC was instructed to examine cybersecurity

---

[75] State of Illinois, 2011

[76] Illinois Commerce Commission, no date

[77] State of Maine, 2010

[78] State of Maine, 2012

and privacy requirements under state and federal law to identify regulatory gaps. The commission was also instructed to develop recommendations to close these gaps and to actively monitor ongoing cybersecurity efforts at the federal level.

1.16.7. Maryland

Maryland has a Commission on Maryland Cybersecurity Innovation and Excellence that focuses on promoting cybersecurity developments within the state. The commission monitors state and federal cybersecurity laws, and provides recommendations for recovery and response plans. The commission was also tasked with a review of policies, standards, and best practices for public utilities. To further promote cybersecurity business interests, the state has created a Cybersecurity Investment Fund to support early-stage cybersecurity technologies and companies. Maryland offers a tax credit for cybersecurity investments.

1.16.8. Ohio

Ohio created the Cybersecurity, Education, and Economic Development Council in 2012. The twelve-member council was to study the state's cybersecurity operations and how the state's cybersecurity industry could be promoted. In 2014, Ohio's HB 483 created the Office of Information Technology within the Department of Administrative Services, and rolled the functions of the Cybersecurity, Education, and Economic Development Council into that office.

1.16.9. Oklahoma

Oklahoma's legislature found that, while AMI technologies offer substantial benefits to customers, they might also pose dangers. The legislature enacted the Electric Usage Data Protection Act to control access to and use of usage data.[79] Utilities must maintain the confidentiality of customers' information, and any third party that consumer information is disclosed to must maintain the security and confidentiality of customer information. Utilities cannot share identifiable customer usage information without consent from the customer.

1.16.10. Pennsylvania

The PAPUC annually reviews the cybersecurity plans of its utilities through self-certification forms.[80] These self-certification forms are confidential, and the Pennsylvania legislature protected the confidential filings of its utilities with the Public Utility Confidential Security Information Disclosure Act of 2006. Utilities have the responsibility to identify when their filings contain confidential information, and all filings marked "Confidential Security Information" are not subject to Pennsylvania's Right-to-Know law. Under this law, state agencies are permitted to develop filing protocols and procedures for public utilities to submit records containing confidential security information. In compliance with Pennsylvania's regulations, utilities' security information is housed with the utility but must be made available

---

79 State of Oklahoma, 2011

80 52 Pa. Code §§101.3 and 101.4.

for inspection by the Commission. PA's multi-disciplinary cybersecurity team has developed a collaborative and compliance assistance oriented approach. The team reviews current regulatory, statutory, and best practices efforts and works to identify ongoing training opportunities for jurisdictional and non-jurisdictional industry as well as Commission staff.

The PAPUC enacted its *Smart Meter Procurement and Installation Implementation* Order at Docket No. M-2009-2092655, entered June 24, 2009, which in part require utilities to adhere to widely-accepted industry and communications standards for providing consumers access to smart meter data in a manner that preserves the integrity, reliability, and security of the grid, distribution system and consumer data.

1.16.11. Texas

Texas established a state Cybersecurity Coordinator in October 2013. The coordinator may implement a voluntary cybersecurity seal of approval program, and is also responsible for the implementation of recommendations made by Texas' Cybersecurity, Education, and Economic Development Council. That council, formed in 2011, is a public-private partnership intent on improving cybersecurity operations of Texas' state government and industry.[81]

1.16.12. Vermont

Under Vermont law, the Commissioner of Public Service must report on savings realized by smart meters and any associated cybersecurity breaches.[82] The Commissioner has the power to request data from electric companies to compile this report, and must submit the report to a number of State legislative committees.

1.17. Industry Organizations

Utilities have emphasized the importance of voluntary standards, and have therefore created their own cybersecurity guidelines. These guidelines create a range of obligations: the requirements in the nuclear industry are mandatory; the water industry offers liability limitations; and the electric industry offers principles for cybersecurity policy. Utility organizations such as the American Water Works Association, the American Gas Association, the American Petroleum Institute, the Edison Electric Institute, and the Nuclear Energy Institute offer guidance on cybersecurity policy to their member utilities. Each of these groups customizes general cybersecurity advice to apply particularly to their utility sector, and their principles can specify to commissions and utilities what aspects of cybersecurity they should focus on.

1.17.1. American Water Works Association

The American Water Works Association (AWWA) has developed a cybersecurity guide for water utilities. These recommendations keep both the current and future world of

---

[81] Texas Department of Information Resources, 2013

[82] State of Vermont, 2012

cybersecurity in mind, and are intended to evolve with time. AWWA developed a *Roadmap to Secure Control Systems in the Water Sector* in 2008, which focused on cybersecurity of ICS.[83] The roadmap recommended practices, outreach, training, certifications, patches, technologies, change management, information exchange, and implementation. AWWA's *Process Control System Security Guidance for the Water Sector* identifies recommendation in a number of categories, including governance and risk management; business continuity and disaster recovery; server and workstation hardening; access control; application security; encryption; telecommunications, network security, and architecture; physical security of process control system (PCS) equipment; service level agreements; operations security; education; and personnel security.[84]

AWWA has also worked with the American National Standards Institute (ANSI) to develop a number of cybersecurity standards for water utilities. Two of these standards, G430-09 and J100-10, have received SAFETY Act designation from DHS, meaning that implementing these standards limits liability a utility may face after a cyber event. G430-09: Security Practices for Operations and Management defines minimum requirements for water or wastewater utilities, and applies to such utilities. G430-09 does not focus primarily on cybersecurity, but does contain some cybersecurity measures, such as access controls.[85] J100-10: Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management for Water and Wastewater Systems offers water utilities a process to identify security weaknesses. J100-10 includes procedures for assessing cybersecurity risks, and for appropriately allocating resources to mitigate the threat.[86]

1.17.2. American Gas Association

The American Gas Association (AGA) contributes to national cybersecurity discussions through its membership in the Oil and Natural Gas Sector Coordinating Council (ONG SCC). AGA encourages its members to participate in its Natural Gas Security Committee, which features a Cybersecurity Task Group. AGA has also developed reports for pipeline operators, including *Cryptographic Protection of SCADA Communications*, a four-part study of SCADA cybersecurity.

1.17.3. American Petroleum Institute

The American Petroleum Institute (API) represents American oil and natural gas companies. API is also a member of the ONG SCC. API hosts an annual Cybersecurity Conference and Expo, where security professionals in the oil and natural gas fields can learn about cybersecurity. The conference intends to provide the latest updates to the cybersecurity threats and mitigation technologies an oil or natural gas company may encounter. API offers *API*

---

[83] American Water Works Association, 2008

[84] American Water Works Association, 2014

[85] American Water Works Association, no date

[86] American Water Works Association, no date

Standard 1164: *Pipeline SCADA Security*, which includes best practices for reviewing and developing SCADA system cybersecurity programs. API recommends that its cybersecurity standard be considered as part of a larger SCADA upgrade project in order to "design in" cybersecurity measures.[87]

1.17.4. Edison Electric Institute

The Edison Electric Institute (EEI) represents investor owned utilities and has worked with federal agencies to develop a number of cybersecurity measures. EEI stresses the importance of DHS' information sharing initiatives, including ES-ISAC, NCCIC, and ESCC. EEI has developed a Threat Scenario Project that helps its member utilities identify threats and mitigation practices. The organization has also been involved in a number of federal initiatives, including the National Infrastructure Advisory Council's *A Framework for Establishing Critical Infrastructure Resilience Goals*, DOE and DHS' Electricity Subsector Cybersecurity Capability Maturity Model and *Roadmap to Secure Control Systems in the Energy Sector*, and the Electricity Subsector Cybersecurity Risk Management Process with DOE, NIST, and NERC.[88]

EEI has also published a series of cybersecurity principles for electric utilities. The principles focus on the reliability impacts of cybersecurity; the coordinated effort needed between electric companies, suppliers of grid components, and the federal government; and the importance of public-private partnerships. EEI recommends that cybersecurity policy recognizes the prioritization of assets; threats be treated differently than vulnerabilities; regulatory structure should be clear; new risks should be proactively managed; both bulk electric and distribution assets should be protected; and emergency-related liabilities should be protected and costs should be recovered from the rate base.[89]

1.17.5. Nuclear Energy Institute

The Nuclear Energy Institute (NEI) has worked extensively with NRC to develop cybersecurity standards and programs. NEI developed a cybersecurity program in 2006, and the nuclear energy industry had entirely adopted the program by 2008.[90] NRC now enforces the implementation of cybersecurity programs, and NEI continues to work with NRC, FERC, and NERC to develop cybersecurity policies. The nuclear industry's cybersecurity policies focus on isolating essential systems with "air-gaps;" strict controls for portable equipment; increased defenses against insider threats; additional cybersecurity controls on equipment most essential for public health and safety; and measures to maintain ongoing effective cyber protection.[91]

---

87 American Petroleum Institute, 2009

88 Edison Electric Institute, 2013

89 Edison Electric Institute, no date

90 Nuclear Energy Institute, 2014

91 Nuclear Energy Institute, 2014

1.17.6. Utilities Telecom Council

The Utilities Telecom Council (UTC) offers tools and information about cybersecurity measures to owners of critical telecommunications systems. UTC is involved in a number of cybersecurity standards, and expresses a desire for "reducing duplication and facilitating harmonization of standards to help our members streamline their cybersecurity policy and standards implementation."[92] The organization offers educational programs and events on a wide range of topics within the cybersecurity field, and has provided cybersecurity updates since November 2012. UTC is also developing practical tools along with government agencies, standards bodies, and other critical infrastructure industry associations.

1.18. Regional Transmission Organizations and Independent System Operators [93]

Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) also consider cybersecurity measures to be a critical part of their system reliability responsibilities. RTOs and ISOs are subject to the NERC CIP standards, and have also implemented other industry standards, guidelines, and frameworks. RTOs and ISOs have utilized the Computer Security Resource Center's Special Publication 800 series and the International Organization for Standardization/International Electrotechnical Commission 2700 series frameworks, as well as technical standards such as NIST's Security Content Automation Protocol and Common Vulnerabilities and Exposures/Common Vulnerability Scoring System.[94]

RTOs and ISOs have, like many other organizations, participated in information sharing groups coordinated by DHS, DOE, and NERC. Further, RTOs and ISOs have coordinated with each other through the ISO/RTO Council (IRC) and the IRC's Security Working Group. RTOs and ISOs must report cybersecurity information to the FBI, ES-ISAC, NERC, and DOE.

RTOs and ISOs have made efforts to assess their cyber defenses. Through metrics developed around resources such as the Lockheed Martin Cyber Kill Chain, RTOs and ISOs have identified and improved system weaknesses. RTOs and ISOs also conduct penetration testing and vulnerability assessments on an annual basis. Education and training has also improved employee awareness of cybersecurity issues, resulting in better defense against attacks such as spear-phishing.

Still, RTOs and ISOs face similar issues to all involved in critical infrastructure cybersecurity. The IRC has identified major challenges in cybersecurity, which include timely access to actionable intelligence associated with ongoing threats, information on effective operational and defensive tradecraft, the limited number of computer network defense

---

92 Utilities Telecom Council, 2014

93 Due to security considerations, representatives from RTOs and ISOs requested that their cybersecurity policies be summarized without identifying the specific RTO or ISO that utilizes that standard or process.

94 ISO/RTO Council, 2013

professionals, and the limited resources available for site-specific security analyses and cybersecurity research.[95]

Trends in Commission Actions

Cybersecurity considerations by state utility commissions undertaken thus far have been limited, but continue to expand. Currently, fifteen commissions have adopted cybersecurity rules or opened cybersecurity dockets. Those commissions that have taken action have not yet had time to evaluate their procedures. As more commissions develop rules and regulations, new regulatory practices may develop, and commissions may revise current regulations. Regulators looking to implement a set of best practices for their cybersecurity considerations may be able to initiate or update a cybersecurity program from these limited sources of comparison.

However, a number of commissions have taken similar approaches to cybersecurity. Commissions have not yet fully developed a standard set of best practices, but there are identifiable trends in state utility cybersecurity regulations. While one individual commission may not have undertaken each of these actions, the trends detailed here represent actions taken by one or more state utility commissions and offer other commissions options they may wish to consider.

Commissions have focused on cybersecurity in the forms of system protection, reliability, and resiliency. When system reliability is the focus, commissions have required incident reporting or cybersecurity audits. Commissions have placed emphasis on the protection of SCADA systems, and requirements on the storage and usage of customers' private information in smart grid deployment initiatives. Some commissions require annual smart grid reports that include cybersecurity considerations. Commissions with ongoing smart grid dockets have asked their utilities how they plan to address cybersecurity and privacy concerns in their ongoing smart grid deployments.

Commissioners and commission staff have completed basic cybersecurity training. These trainings have detailed the basics of cybersecurity, such as safe internet usage or cyber hygiene, as well as areas specific to utility regulation, such as information sharing and incident response coordination. In addition to training, commission staffs have continued to monitor developments in technology. This included new areas of vulnerability and commonly used information technology.

Similarly, commissions have remained aware of changes that can affect best practices and standards. Commission staffs monitor and participate in the development of NIST's cybersecurity framework and NERC's CIP standards. Commission staffs, as well as other state government officials, have kept aware of cyber threats and developments through continued interaction with DHS and their states' law enforcement and technology offices. Commission representatives have also participated in a number of training exercises intended to provide the critical infrastructure community with realistic scenarios and the opportunity to test responses.

---

[95] ISO/RTO Council, 2013

Commissions have exempted cybersecurity discussions from the public record. Where allowed by statute, commissions encourage their regulated utilities to have confidential conversations detailing the utility's response plan and technical capabilities. Information about a utility's cybersecurity plan should not be made public, as to avoid exposing a utility's cybersecurity responses to attackers. In some states, additional legislation has been needed to ensure the confidentiality of a utility's cybersecurity plans.

Commissions have examined the frameworks produced by NIST and other utility organizations in order to develop applications for their frameworks. Some commissions have asked themselves and their utilities how these documents can be applied to their states' critical infrastructure and other utility assets under the jurisdiction of state utility commissions.

Commissions examining their responsibilities can consider any number of these actions, and should evaluate them within their regulatory context. In that process, commissions should remain open to new ideas, and keep in mind that state legislation plays a large role in determining their available options. Answering the following questions can provide guidance for commission actions:

- Can your commission keep security information confidential from the public?
- Has your commission been instructed to examine smart grid technologies?
- Has your commission been instructed to examine cybersecurity initiatives for all critical utility infrastructures within your state?
- Do your reliability standards include cybersecurity considerations?
- Are there incident response exercises that your utilities participate in that you could join?
- Can your staff participate in the development of frameworks or standards?
- Do frameworks produced by standards or industry groups apply to your utilities or jurisdiction?
- Is there education available that will enable commission staff to make prudency evaluations and recommendations regarding expenditures?
- Is there training or education available to enable commission staff to evaluate the effectiveness of a utility's cybersecurity plans?

State utility commissions, as a part of the larger critical infrastructure community, play a key role in ensuring the safety and reliability of the United States' utility services. Cybersecurity considerations are an important piece of that responsibility, and commissions will continue to develop rules and regulations focused on customer privacy and system reliability.

Bibliography

Albright, David, Paul Brannan, and Christina Walrond. *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Washington, DC: Institute for Science and International Security, 2011.

American Petroleum Institute. "API Standard 1164: Pipeline SCADA Security." June 2009. Web. 21 Aug. 2014.

American Water Works Association. Process Control System Security Guidance for the Water Sector. 2014. Denver, CO.

_____. "Risk and Resilience Management of Water and Wastewater Systems (RAMCAP)." Web. 1 Aug. 2014.

_____. *Roadmap to Secure Control Systems in the Water Sector*. Denver, CO: American Water Works Association, 2008. Web. 1 Aug. 2014.

_____. "Security Practices for Operations and Management." Web. 1 Aug. 2014.

Arkansas Public Service Commission. "Order Number 8." 3 Aug. 2011. Web. 8 Aug. 2014.

Behr, Peter and Blake Sobczak. "With No Staff and 'Very Little or No Cybersecurity Standards,' States Ill-Equipped to Face Threats." *EnergyWire* 5 May 2014. Web. 13 Aug. 2014.

California Public Utilities Commission. *Annual Report to the Governor and the Legislature: California Smart Grid*. San Francisco, CA: California Public Utilities Commission, 2014. Web. 21 Aug. 2014. Smart Grid Report.

_____. "Decision 11-07-056." 29 July 2011. Web. 21 Aug. 2014.

Clayton, Blake and Adam Segal. *Addressing Cyber Threats to Oil and Gas Suppliers*. New York, NY: Council on Foreign Relations, 2013.

Clinton, Bill. "Presidential Decision Directive/NSC-63." 22 May 1998. Web. 5 Aug. 2014.

Colorado Smart Grid Task Force. *Deploying Smart Grid in Colorado: Recommendations and Options*. Denver, CO: Colorado Smart Grid Task Force.

Communications Security, Reliability and Interoperability Council. *Final Report: Consensus Cyber Security Controls*. Washington, DC: Communications Security, Reliability and Interoperability Council, 2013.

Curry, Kimberly A. and Douglas E. Micheel. "Joint Utility Cyber-Security Process Reporting Plan." 14 Nov. 2012. Web. 6 Aug. 2014.

Department of Homeland Security. "Cyber Storm: Securing Cyber Space." N.p., n.d. Web. 1 Aug. 2014.

Edison Electric Institute. "EEI Principles for Cybersecurity and Critical Infrastructure Protection." Web. 4 Aug. 2014.

_____. "Electric Power Industry Initiatives to Protect the Nation's Grid from Cyber Threats." Jan. 2013. Web. 4 Aug. 2014.

Fischer, Eric A. Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions. Washington, DC: Congressional Research Service, 2013.

Germano, Judith H. and Zachary K. Goldman. *After the Breach: Cybersecurity Liability Risk*. New York, NY: Center on Law and Security: New York University School of Law, 2014. Web. 5 Aug. 2014.

Homeland Security News Wire. "States Lack Expertise, Staff to Deal with Cyberthreats to Utilities." *Homeland Security News Wire* 8 May 2014. Web. 13 Aug. 2014.

House, Arthur. *Cybersecurity and Connecticut's Public Utilities*. New Britain, CT: Connecticut Public Utilities Regulatory Authority, 14 Apr. 2014.

Illinois Commerce Commission. "Electric Infrastructure Investment Plans." Web. 31 July 2014.

Indiana Utility Regulatory Commission. "Order of the Commission." 14 Mar. 2013. Web. 8 Aug. 2014.

ISO/RTO Council. *Response of the ISO/RTO Council to National Institute of Standards and Technology's February 26, 2013 Request for Information*. ISO/RTO Council. Apr. 2013.

Kentucky Public Service Commission. "Commission Staff's First Request for Information." 27 Feb. 2013. Web. 11 Aug. 2014.

_____. "Order Regarding Request for Confidential Treatment." 1 Apr. 2014. Web. 11 Aug. 2014.

Keogh, Miles and Christina Cody. *Cybersecurity for State Regulators 2.0*. Washington, DC: National Association of Regulatory Utility Commissioners, 2013.

Lichtenberg, Sherry. *Smart Grid Data: Must There Be Conflict Between Energy Management and Consumer Privacy?* Silver Spring, MD: National Regulatory Research Institute, 2010.

Louisiana Public Service Commission. "Official Bulletin #1030." 15 Feb. 2013. Web. 6 Aug. 2014.

_____. "RFP 14-05: Louisiana Public Service Commission Request for Proposal." 3 Mar. 2014. Web. 6 Aug. 2014.

Malashenko, Elizaveta, Chris Villarreal, and J. David Erickson. *Cybersecurity and the Evolving Role of State Regulation: How It Impacts the California Public Utilities Commission*. San Francisco, CA: California Public Utilities Commission, 2012. Web. 13 Aug. 2014. Grid Planning and Reliability Policy Paper.

Massachusetts Department of Public Utilities. "Investigation by the Department of Public Utilities on Its Own Motion into Modernization of the Electric Grid." 23 Dec. 2013. Web. 12 Aug. 2014.

_____. "Investigation by the Department of Public Utilities on Its Own Motion into Modernization of the Electric Grid: Vote and Order Opening Investigation." 2 Oct. 2012. Web. 12 Aug. 2014.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: National Institute of Standards and Technology, 2014. Web. 31 July 2014.

_____. NIST Roadmap for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD.

New Jersey Board of Public Utilities. "In the Matter of Cyber Incident Reporting for Utility

Industrial Control Systems." 13 Oct. 2011. Web. 6 Aug. 2014.

North American Electric Reliability Corporation. *2011 NERC Grid Security Exercise: After Action Report*. 2012a. Washington, DC.

_____. *Grid Security Exercise (GridEx II): After-Action Report*. 2014. Washington, DC.

_____. *Electricity Sub-Sector Coordinating Council Charter*. 2012b. Atlanta, GA.

Nuclear Energy Institute. Cyber Security Strictly Regulated by NRC; No Additional Regulation Needed. 2014. Washington, DC.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. 1997. Washington, DC.

Ponemon Institute LLC. *Critical Infrastructure: Security Preparedness and Maturity*. Unisys, 2014. Web. 23 Aug. 2014.

Public Service Commission of the District of Columbia. "Order Number 17373." 6 Feb. 2014. Web. 11 Aug. 2014.

Rivaldo, Alan. *Report on Electric Grid Cybersecurity in Texas*. Austin, TX: Public Utility Commission of Texas, 2012. Web. 21 Aug. 2014.

Santa, Donald F. *INGAA Responds to Senator Rockefeller on Cybersecurity Legislation*. 15 Oct. 2012. Web. 28 Aug. 2014.

State of California. Electrical Consumption Data; Local Publicly Owned Electric Utility Prohibited from Sharing, Disclosing, or Making Accessible to Third Party; Exceptions; Disclosure of Use of Data by Third Party for Secondary Commercial Purpose; Security Procedures and Practices; Voluntary Disclosure by Customer to Unaffiliated Third Party. Vol. 8381. N.p., 2012. Print.

State of Colorado. Colorado Smart Grid Task Force--Fund--Definition--Reports--Repeal. N.p., 2012. Print.

State of Illinois. Provisions Relating to the Smart Grid Advanced Metering Infrastructure Deployment Plan. N.p., 2011. Print.

State of Maine. Declaration of Policy on Smart Grid Infrastructure. Vol. 3143. N.p., 2010. Print.

_____. Resolve, To Examine Cyber Security and Privacy Issues Relating to Smart Meters. Vol. 0439. N.p., 2012. 04.

State of New York Public Service Commission. "Order Instituting Proceeding." 24 Apr. 2014. Web. 11 Aug. 2014.

State of Oklahoma. *Electric Usage Data Protection Act*. N.p., 2011. Print.

State of Pennsylvania. "Confidential Security Information." Web. 7 Aug. 2014.

_____. "Public Utility Preparedness Through Self Certification." Web. 7 Aug. 2014.

State of Vermont. *Smart Meters; Customer Rights; Reports*. N.p., 2012. Print.

Scarfone, Karen, Wayne Jansen, and Miles Tracy. *Guide to General Server Security*. Gaithersburg, MD: National Institute of Standards and Technology, 2008.

Technologies Subgroup. “Current Thinking.” NYS DPS - Platform Technology Working Group. 2014.

Texas Department of Information Resources. “Technology Brief: Cybersecurity.” Web documents - Undefined. N.p., 28 Feb. 2013. Web. 31 July 2014.

The Public Service Commission of Maryland. “Order No. 83571.” 2 Sept. 2010. Web. 6 Aug. 2014.

_____. “Order No. 85680.” 21 June 2013. Web. 6 Aug. 2014.

The Public Service Commission of the State of Missouri. “Order Directing Notice and Directing Filing.” 17 July 2012. Web. 6 Aug. 2014.

Transportation Security Administration. “TSA Pipeline Security Guidelines.” Apr. 2011. Web. 21 Aug. 2014.

United States Department of Commerce. “Discussion of Recommendations to the President on Incentive for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program.” 2013. Web. 5 Aug. 2014.

United States Environmental Protection Agency. *Cyber Security 101 for Water Utilities*. 2008. Washington, DC.

United States Nuclear Regulatory Commission. “Backgrounder on Cyber Security.” Apr. 2010. Web. 4 Aug. 2014.

_____. Nuclear Regulatory Legislation. 2013. Washington, DC.

_____. “Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities.” Jan. 2010. Web. 4 Aug. 2014.

Utilities Telecom Council. “Cybersecurity.” *Utilities Telecom Council*. N.p., 2014. Web. 21 Aug. 2014

Washington Utilities and Transportation Commission. “Docket U-090222, General Order R-559.” 24 March. 2010. Web. 21 Aug. 2014.

Wilson, Raymond. *Energy Assurance Plan (Final/Draft)*. New Britain, CT: Connecticut Department of Energy and Environmental Protection, Aug. 2012.

Appendix A

Middle Atlantic Cybersecurity Collaborative

(State Utility Commissions)

"We move that the Middle Atlantic Collaborative contact NRRI requesting that NRRI study what the responsibility of state commissions is vis-à-vis cyber security, how different state commissions (legislatures) have addressed their regulatory responsibilities (rules/regulations, staff training, other actions) and set forth best practices for a state commission to effectively exercise their regulatory responsibilities over cyber security" (September 2014).

Chairs/Commissioners

- Hon. Joanne Doddy Fort, Commissioner, District of Columbia PSC
- Hon. Asim Haque, Commissioner, PUC of Ohio
- Hon. Ann Hoskins, Commissioner, Maryland PSC
- Hon. Kevin Hughes, Chairman, Maryland PSC
- Hon. Betty Ann Kane, Chairman, District of Columbia PSC
- Hon. Robert Powelson, Chairman, Pennsylvania PUC
- Hon. Dianne Solomon, Commissioner, New Jersey BPU
- Hon. Dallas Winslow, Chairman, Delaware PSC
- Hon. Pamela Witmer, Commissioner, Pennsylvania PUC

Commission Staff

- Rachael Brekke, New Jersey BPU
- Lois Burns, Pennsylvania PUC
- Patrick McDonnell, Pennsylvania PUC
- Thomas Pearce, PUC of Ohio
- Ron Teixeira, Delaware PSC
- Ellen Vancko, Maryland PSC