PHASE 1 REPORT

IMPROVING THE CYBERSECURITY OF THE ELECTRIC DISTRIBUTION GRID

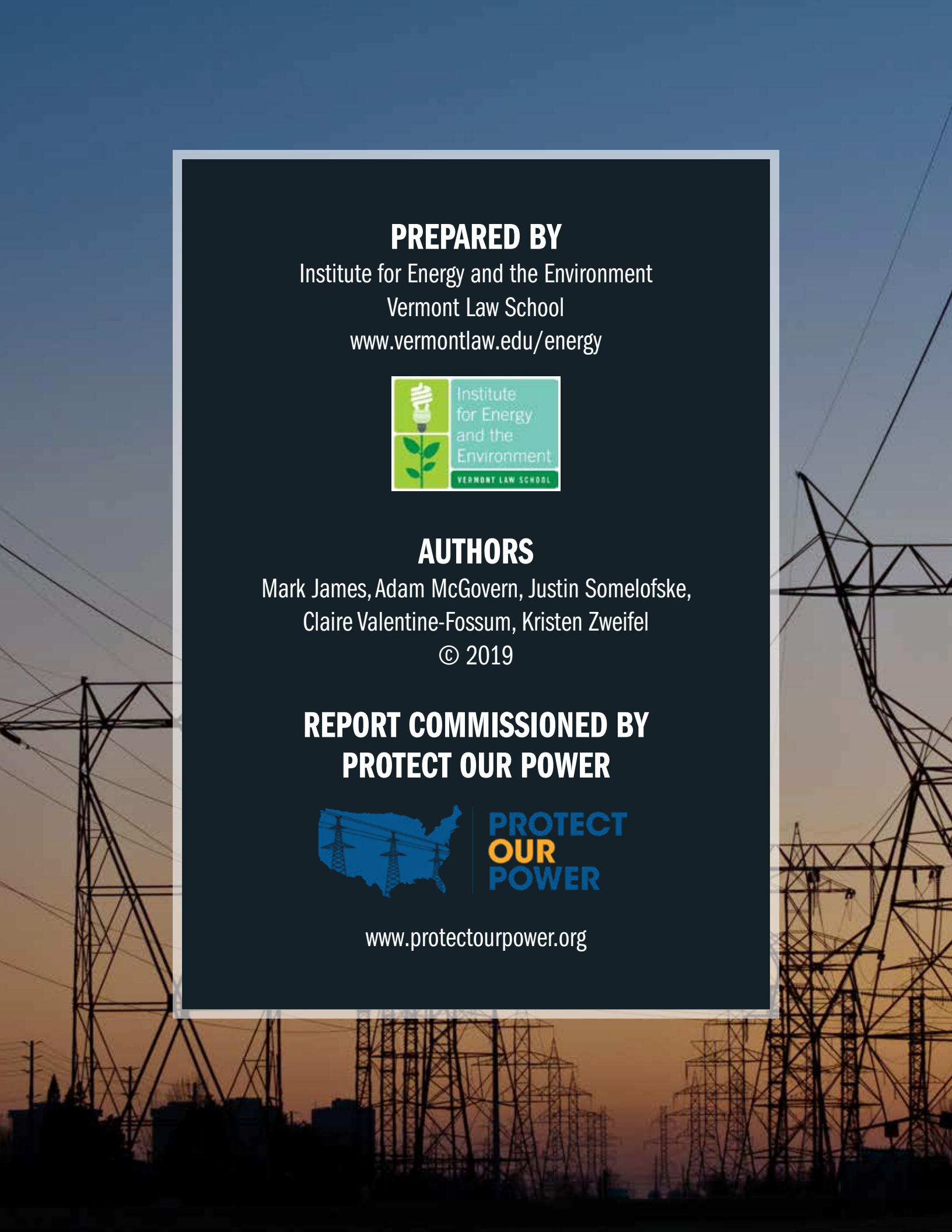
Identifying Obstacles and Presenting Best Practices for Enhanced Grid Security

Institute for Energy and the Environment
VERMONT LAW SCHOOL

VERMONT LAW SCHOOL

PROTECT OUR POWER

Institute for Energy and the Environment, Vermont Law School | APRIL 2019



PREPARED BY

Institute for Energy and the Environment
Vermont Law School
www.vermontlaw.edu/energy

AUTHORS

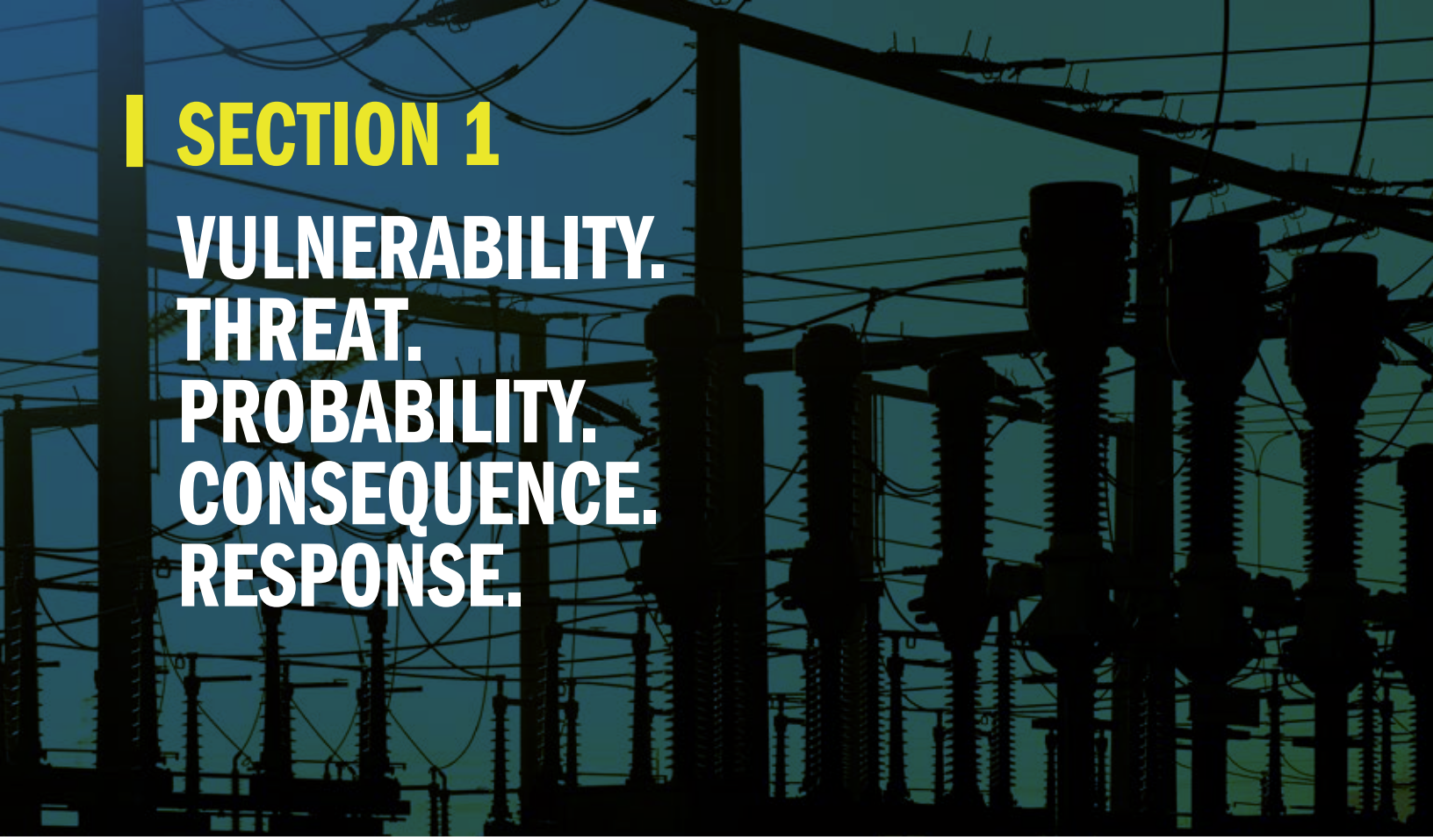
Mark James, Adam McGovern, Justin Somelofske,
Claire Valentine-Fossum, Kristen Zweifel

REPORT COMMISSIONED BY PROTECT OUR POWER

PROTECT OUR POWER

www.protectourpower.org

TABLE OF CONTENTS



SECTION 1

VULNERABILITY. THREAT. PROBABILITY. CONSEQUENCE. RESPONSE.

electricity over 5.5 million miles of distribution lines to customers. Hundreds of millions of moving, interconnected pieces working in concert to make sure that the lights stay on. However, the sheer size of the system makes it difficult to defend against all attacks.

The vulnerability of our electric system increases as the potential attack surface of our electric system grows. Increases in automation, growth in the number and type of distributed energy resources, and the convergence of enterprise information technology (IT) and operations technology (OT) are producing a larger attack surface that must be protected against intrusion and attack. The distribution system constitutes 80-90% of all grid infrastructure and is the focal point for many parts of the evolving nature of electricity generation and distribution. A National Academy of Sciences report highlighted the rigidity of the electricity system and its inability to withstand or quickly recover from attacks on multiple components.[1] Adding millions of internet-connected home appliances to the grid management operations is creating new and unexpected points of access to a grid that was designed for a unidirectional utility-customer relationship. The pace of connections is accelerating which adds impetus to resolving obstacles now.

Adding to the complexity is the distribution utilities come in multiple sizes and business models. A distribution utility can serve a thousand customers or a million customers; it can be investor-owner, a membership cooperative, or a public power utility; it might be part of a larger FERC-regulated entity, subject to state commission jurisdiction, or responsive only to its members or elected officials; it might have dedicated cybersecurity staff or it might be reliant on external expertise. The diversity is a strength, but it raises difficulty in crafting a unified response. This report addresses some of the fundamental concepts that can be

1 National Academy of Sciences, Terrorism and the Electric Power Grid (2012) at 1.

deployed across a variety of utilities.

Threat

Every day brings more reports on new and emerging threats to the electricity system. Recent attacks in Ukraine demonstrated that distribution systems are ripe for targeting. The targeting of distribution systems is not a problem that exists only outside the United States. The ICS-CERT report noted that there were more than 270 cyber emergencies within the U.S. energy sector from the period of 2013-2015. In fact, the energy sector was targeted more than any other sector.[2]

The sophistication of threat actors continues to grow as well. The capability and capacity of cybercrime groups and nation states increases every day and their focus on critical infrastructure systems is becoming more acute. The Director of National Intelligence's Worldwide Threat Assessment recently stated that China and Russia have the capability to cause localized, temporary disruptions to U.S. gas and electricity distribution systems.[3] More concerning is that the Assessment reports that Russia is actively mapping American critical infrastructure systems "with the long term goal of being able to cause substantial damage."[4]

2 U.S. Department of Energy, Multiyear Plan for Energy Sector Cybersecurity, March 2018 at 9.

3 Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, January 29, 2019 at 5.

4 *Id.* at 6.

Probability

The probability of an attack continues to grow. A recent survey of utility executives indicates almost half of them believe that that most important question is not "if" a cyberattack will occur but "when" it will occur.[5] Large utilities are experiencing millions of attempts per day by parties seeking to gain access to their business enterprise and operations systems. The Tennessee Valley Authority, which supplies electricity to more than 10 million people in seven different states,[6] is seeing an increased number of penetration attempts.[7] Connecticut utilities see upwards of a million daily attempts to penetrate and compromise their systems.[8] The same utility executives that are certain that an attack is imminent, also believe that their systems do not prevent all attack attempts.[9] It is worrisome that the initial point of penetration may only be platform that gives access to the intended target which turns every utility into a potential point of access, whether they serve 1000 customers or 5 million customers. Access to business enterprise systems can give entry into industrial control systems and operating systems. A small phishing attempt may be the opening move in a longer lasting and farther-reaching attempt to disrupt the grid. Moreover, attackers can inhabit a system for months, learning and mapping the movement of information and the levers of control. Penetrating the control systems of a distribution utility may create an access point into the bulk power system.

Consequence

The consequence of a widespread cyberattack on the distribution system would be crippling to the U.S economy and create danger for the population. Unlike attacks on an information technology system, a cyberattack on industrial control systems and operating systems has the potential to disrupt power and fuel supplies and threaten human health and safety.[10] Furthermore, a coordinated attack on multiple distribution system control centers and substation could have the same impact as an attack on the bulk power system.[11] Electricity is the common link binding together the other 15 federal critical infrastructure sectors. Our electricity system is connected to our natural gas, water, communications, and fuel distribution systems.[12] A prolonged loss of electricity would interfere with the delivery of other critical services.

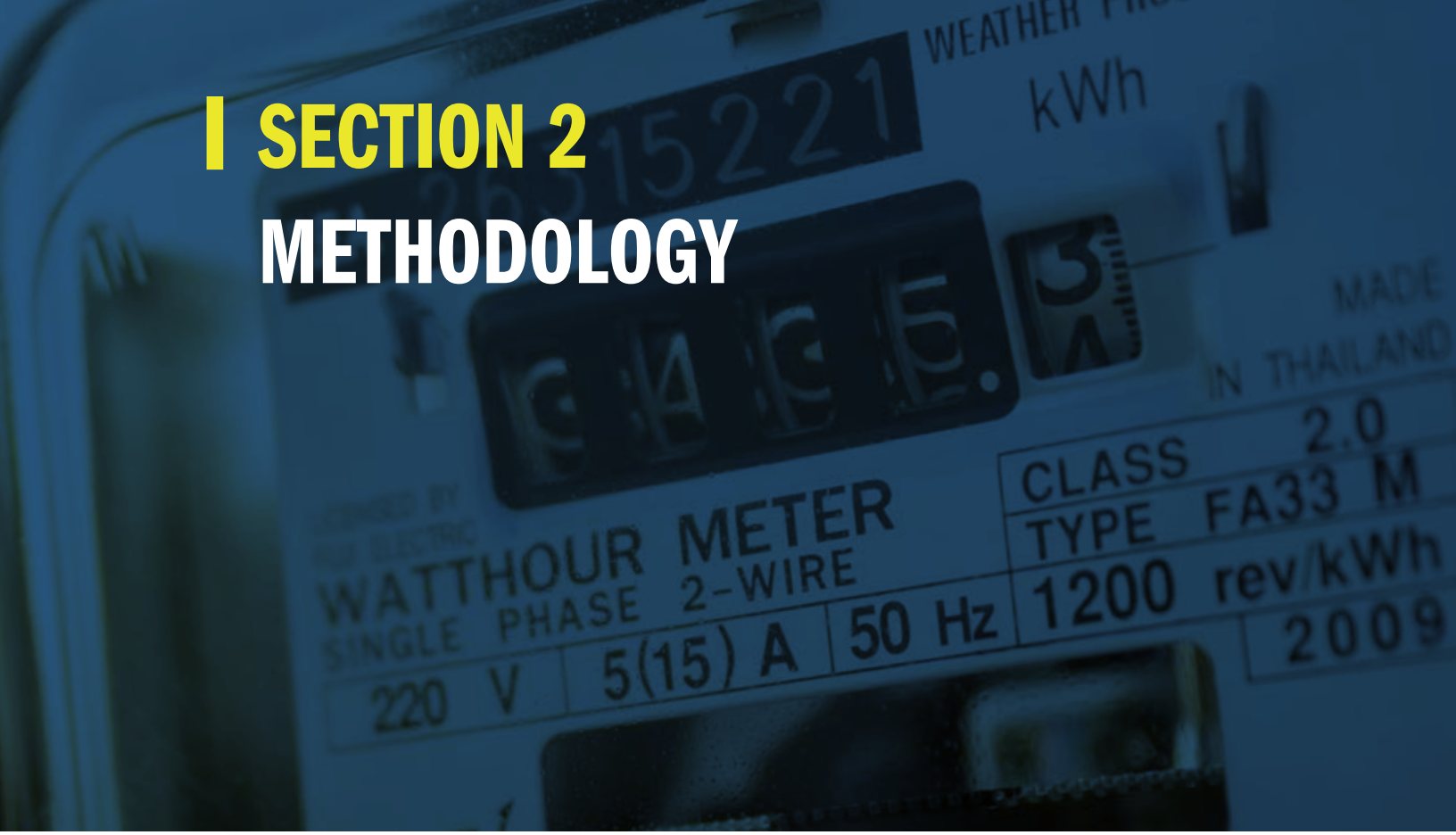
Estimates of the potential economic damage of a cyberattack are staggering. The current number of annual outages, which overwhelmingly occur on the distribution system, costs the U.S. economy upwards of a $100 billion/year. Lloyd's of London estimates that a coordinated cyberattack on the east coast of the United States could cost upwards of $243 billion in insurance costs alone and it would result in loss of life and damage to the environment.[13]

5 KPMG, 2018 KPMG CEO Outlook: Power and Utilities, November 2018, https://home.kpmg.com/xx/en/home/insights/2018/09/2018-kpmg-ceo-outlook-power-and-utilities.html.
6 Tennessee Valley Authority, About TVA, https://www.tva.gov/About-TVA.
7 Tennessee Valley Authority, Cybersecurity: The New First Line of Defense, https://www.tva.gov/Newsroom/Cybersecurity-The-New-First-Line-of-Defense.
8 Connecticut Public Utilities Regulatory Agency, Connecticut Critical Infrastructure 2018 Annual Report (2018) at 2.
9 *Supra* note 5.
10 *Supra* note 2 at 8.
11 University of Illinois at Urbana-Champaign, NextGrid Illinois: Utility of the Future Study (2018) at 81.
12 Advanced Energy Economy Institute, Cybersecurity in a Distributed Energy Future (2018) at 1.
13 University of Cambridge, Centre for Risk Studies, The insurance implications of a cyber attack on the US power grid (2015) at 21.

Response

Is there a single solution to mitigate this threat? No. As with many complex problems, many coordinated small steps are the best way of making progress. Increased attention, financial resources, and planning for cybersecurity will be critical to reducing vulnerabilities. We know that utilities and utility commission will be at the center of those efforts in proposing and evaluating cybersecurity and grid resilience enhancements to the distribution grid. A resilient system can only emerge from a coordinated forward-thinking response to address threats and vulnerabilities.

What are the steps that can be taken now? Utility commissions must press forward in key areas to build and strengthen relationships with their regulated and non-regulated utilities, to evaluate traditional cost recovery mechanisms to determine if they align with system security goals, and to consider what metrics are needed to evaluate utility investments and system performance. Utilities and other stakeholders must be engaged partners in all facets of this process. This report seeks to push along discussions in these areas by highlighting key questions and identifying best practices for utility commissions and utilities. These are small steps in a coordinated response to protecting the grid.



SECTION 2
METHODOLOGY

OUR RESEARCH PROCESS involved interviewing key industry participants and reviewing primary source documents. We interviewed more than 15 entities – investor owned utilities, electric membership cooperatives, public power utilities, national trade organizations, regional organizations, public power utilities, and multiple regulatory commissions. We spoke with CEOs, presidents, vice presidents, chief information security officers, directors of regulatory affairs, regulatory commission staff, former Commissioners, and program directors. We also read commission dockets, state statutes and regulations, trade association papers, industry white papers, third party reports, and news stories. We identified common barriers to improving the cybersecurity posture of distribution utilities. We sought to highlight best practices for addressing these barriers or create a list of discussion questions for utility commissions seeking guidance on how to reduce those barriers.

This report is intended to be an extensive examination of leading utility commission practices and procedures on distribution cybersecurity. This report is not intended to be an exhaustive examination of all utility commission practices and procedures. Our goal is to represent selected examples of state actions to overcome obstacles as it is not possible to cover every action being taken at the state level.

A list of all the individuals interviewed and their organizational representation is included in Appendix 1. In order to facilitate open communication, however, we did not attribute comments directly to specific interviewees. Organizational affiliation of these individuals should not be construed to suggest that any of these organizations support any statements or positions herein described.

SECTION 3

ORIGINS OF CYBERSECURITY ACTIVITY

Key Takeaways

- **No Single Pathway to Starting.** Establishing continuous communication between utilities and their regulatory commissions is the first step to improving the depth and quality of efforts to address cybersecurity vulnerabilities. The utilities, the commission, the legislature, or the governor all can lead. Existing programs have emerged from customer data privacy proceedings, the addition of dedicated staff, or as part of grid modernization efforts.

ACROSS OUR RESEARCH AND INTERVIEWS, we heard the same statement that utilities and utility commissions must do something to address current and future cybersecurity threats. The unanimity of voices urging more and deeper action on cybersecurity broke apart when faced with the question of where to act and how to act. Action is being taken; however, our survey of state public utility commission approaches to cybersecurity reveals that there is no single pathway to address cybersecurity vulnerabilities. State public utility commission action was initiated from within the commission by commissioners or commission staff, by legislative act, and by gubernatorial directive. Some state action evolved from advanced metering infrastructure and smart grid dockets, 9/11 and severe storms triggered some state action, some actions started with customer data privacy concerns before adding in protecting operations technology, and others evolved from increased knowledge of the risks posed by an attack on the grid. The source of the initiating action could vary, but the linking theme was a demonstrated interest in cybersecurity, the commitment of financial and staff resources, and an indication to the utilities of the Commission's long-term investment in this area.

This section explores the history behind the decisions of individual states to address grid resilience and cybersecurity. The section expands the steps used by the states to move into this area with the goal of showing that multiple pathways exist and that there is no single model for becoming a cybersecurity leader. Nor is there a consistent pattern of top-down or bottom-up driven action. What is plain to see is that a commitment by commissions to engage with their regulated utilities and other stakeholders and the allocation of resources need to build capacity and expertise matter is a necessary element. Whether it is a legislature, governor, or commission that initiates action, the responsibility for meeting objectives usually falls upon the commission. It is commissions and commission staff engaging with utilities, educating and training themselves, and finding ways to facilitate and protect disclosures of confidential information.

Case Studies

We selected California, Michigan, and Connecticut[14] as case studies to demonstrate the diversity of approaches available to states and their utility commissions. In California and Michigan, cybersecurity programs emerged from smart grid and AMI proceedings and the states' interests in protecting IOU customer data. Both states have mandatory reporting to the respective commissions on the condition of the electric utilities' cybersecurity protocols. Connecticut took a different approach, starting its efforts at the advice of its commission chairman to the governor to address cybersecurity as a threat to infrastructure and reliability. The advice to the Connecticut governor evolved into a voluntary reporting process under which the commission and other state agencies worked with utilities to develop cybersecurity reporting protocols.

CALIFORNIA

Over the past two decades, California's cybersecurity protection efforts evolved from a concern about customer data privacy into a full-fledged program covering grid operations technology. The CPUC has added new cybersecurity specific requirements, clarified existing requirements, and developed new research programs to address technology gaps. Flexible and adaptable processes have allowed the Commission to evolve to meet new challenges. The California Public Utilities Commission (CPUC) has been the central organization guiding California's extensive cybersecurity program. Overall the last two decades, the California legislature has directed the CPUC to develop programs and lead actions. What can be observed is a pattern of state action that aligns with federal efforts to secure the grid. For example, the CPUC was already engaged in North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) development and actively participating in the development of the Urgent Action Cyber Security Standard 1200 (UA 1200), a NERC CIP predecessor when SB 1386 (Peace) was passed in 2002.[15] SB 1386 required any company with personal information of a Californian to report unauthorized releases of that information.

California aligned its early activities with emerging federal legislation. The passage of Energy Independence and Security Act of 2007 (EISA) and its focus on the smart grid spurred a nation-wide focus on distribution grid cybersecurity. EISA stated that "the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth..."[16] Section 1301 of the EISA described a Smart Grid, among other things as a "dynamic optimization of grid operations and resources, with full

14 There are many states taking action on cybersecurity and this is only a selection of a few of the leading examples. We chose these three states as the Advanced Energy Economy Institute's 2018 Cybersecurity in a Distributed Energy Future report identified California, Michigan, and Connecticut as state leaders in efforts to improve distribution system cybersecurity. Other examples of state actions populate the different sections of this report and can provide insight into options for developing and administering cybersecurity programs.

15 California Public Utilities Commission, Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission (2012) http://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/About_Us/Organization/Divisions/Policy_and_Planning/PPD_Work/Pre_2013_PPD_Work/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf at 18.

16 Energy Independence and Security Act Title XIII at § 1301 (2007).

cyber-security." [17] Section 1306(d) of the EISA defines "smart grid functions," and Section 1307 (a) amended PURPA to require "states to consider imposing certain requirements and authorizing certain expenditures" for smart grid investment.[18] Specifically,

> *"each State shall consider authorizing each electric utility of the State to recover from ratepayers any capital, operating expenditure, or other costs of the electric utility relating to the deployment of a qualified smart grid system, including a reasonable rate of return on the capital expenditures of the electric utility for the deployment of the qualified smart grid system."*[19]

The EISA amended the Public Utility Regulatory Policies Act (PURPA) with a specific obligations of the states to start considering smart grid installation.[20] The CPUC responded by issuing an Order Instituting Rulemaking (R08-12-009) on December 22, 2008.[21] The intent of the order was to give the CPUC to the ability to set policies, standards, and protocols for IOUs "to guide the development of a smart grid system and facilitate integration of new technologies such as distributed generation, storage, demand-side technologies, and electric vehicles"[22] while still protecting ratepayers and industry investment.[23] The Rulemaking also required IOUs to submit an annual Smart Grid Deployment Plan.[24] After the CPUC opened the Rulemaking, the federal government passed the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA amended the §1304(b)(3) subsections of the EISA to require the Secretary of the Treasury to provide financial support for smart grid demonstration projects.[25]

Following Rulemaking 08-12-009 and the ARRA, in April of 2009, the Chair of the California Senate Energy, Utilities, and Communication Committee, Alex Padilla (D)[26] introduced SB17. The bill required the CPUC in consolation with the State Energy Resources Conservation and Development Commission (Energy Commission), the ISO, and other key stakeholders, to develop requirements for a smart grid deployment by July 1, 2010, and each electric corporation to submit to the CPUC a smart grid development plan by July 1, 2011.[27] The Governor approved the bill October 11, 2009, amending Division 4.1 of the Public Utilities Code.[28] The bill's purpose was to require investment into smart grid technology, in

17 Energy Independence and Security Act Title XIII at § 1301(2) (2007).
18 California Public Utilities Commission Rule 08-12-009 at § 2, citing to PURPA § 111(d) (16) http://docs.cpuc.ca.gov/publishedDocs/published/FINAL_DECISION/95608-01.htm#P74_5114.
19 PURPA § 111(d)(16)(B)
20 Energy Independence and Security Act, § 1307(b)(1) amending PURPA § 112(b).
21 California Public Utilities Commission Rule 08-12-009 http://docs.cpuc.ca.gov/publishedDocs/published/FINAL_DECISION/95608.htm.
22 *Id.* at §1.
23 *Id.* at §3.
24 *Id.* at §3. 8.
25 American Recovery and Reinvestment Act of 2009 Title IV at §405 https://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.
26 Currently CA Sec. of State.
27 California Senate Bill 17 (Padilla), Electricity: smart grid systems (2009-2010) at Legislative Counsel's Digest http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200920100SB17.
28 *Id.*

particular advanced meter infrastructure. (AMI).[29] After the bill's passage, in Decision 10-06-047, the CPUC required utilities to specifically include a separate section on cybersecurity in their Smart Grid Deployment plans, rather than include it in the strategic planning section.[30]

After the AMI roll out, the Legislature passed SB1476 (Padilla) to address the fear that "smart meter systems could be subject to hacking, leaving consumers vulnerable to identity theft" by limiting the consumption data and personal information available to a third party.[31] This prompted the CPUC to adopt Decision 10-06-047 on July 28, 2011.[32] The Decision covers the CPUC's jurisdiction over data and data privacy, third party access to customer usage, and specifically requires an IOU to file an annual report outlining its progress on the CPUC Smart Grid Deployment Plan.[33] Additionally, in 2011, The CPUC issued Decision 11-07-056 to provide privacy protections for customer data by regulating third parties with access to customer usage data through the implementation of AMI.

Finally, in 2012, the CPUC Staff published a policy paper titled "Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission."[34] First, Staff noted that federal cyber protections do not reach to the distribution grid, and state regulators should implement cybersecurity measures into the modernization development of the distribution grid.[35] Second, that the CPUC should apply a stringent "risk assessment framework" to General Rate Cases (GRCs) for cybersecurity for IOUs, like the assessment the CPUC developed for pipelines following the 2010 rupture of a PG&E pipeline in San Bruno, California.[36] There the CPUC worked with an Independent Review Panel and the National Transportation Safety Board to develop safety standards.[37] Third, Staff recommended that IOUs include cyber privacy protection for customers in their Smart Grid Deployment Plans.[38] Finally, Staff recommended that the CPUC open an Order Instituting Rulemaking "to further investigate appropriate cybersecurity policies."[39]

The effects of California's long-term investment in cybersecurity are most visible in the response of its regulated utilities. Using PG&E's program as an example, it can be demonstrated how the program can evolve to meet new challenges and address new vulnerabilities. In 2012, PG&E released its Smart Grid Deployment Plan in which it focused on the benefits of smart meter technology for its ratepayers. PG&E noted the technology would help ratepayers manage their energy use to save money and allow PG&E to monitor

29 California Senate Bill 17 (Padilla), Electricity: smart grid systems, Bill Analysis by Chairman Padilla of the "Senate Energy, Utilities and Communications Committee (April 29, 2009) http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB17.

30 *Supra* note 15 at 18.

31 California Senate Bill 1476 (Padilla), Bill Analysis, Senate Judiciary (April 12, 2010) http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB1476.

32 California Public Utilities Commission Decision 10-06-047 (2011) http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/140369.htm.

33 *Id.* at Ordering para.

34 *Supra* note 15.

35 *Supra* note 15 at iii.

36 *Supra* note 15 at iii-iv.

37 *Supra* note 15.

38 *Supra* note 15 at iii-iv.

39 *Supra* note 15 at iii-iv.

the grid for reliability.[40] Additionally, in 2012, PG&E finished its Advanced Detection and Analysis of Persistent Threats cybersecurity project. The project focused on "increasing the Utility's capability to effectively anticipate, prevent, and respond to a new and emerging class of cyber and physical threats known as Advanced Persistent Threats, or APT" to meet NERC-CIP regulatory compliance.[41] The 2012 report also outlined other cybersecurity projects in the works (including CES-21 discussed below). PG&E specifically observed that using "risk assessment can greatly enhance the ability of regulators to determine the appropriate level of funding for cybersecurity measures, recognizing that a 100 percent secure system cannot be achieved."[42] This echoes the 2012 CPUC reliability policy paper, where CPUC "recognized that explicit safety and security risk assessment that includes cybersecurity should become the cornerstone of how the CPUC approaches reliability and safety, particularly through the GRC process."[43] PG&E's 2018 report notes the completion of the ADAPT program, the 4th year of 5 of its CES-21 project, and the Identity and Access Management (IAM) program (which expands PG&E's capabilities to reduce unauthorized access to its systems).[44]

Case Study: CES-21 Project

California regulators and legislators have devoted considerable resources to improving the technology used to protect sensitive systems from emerging threats. The CES-21 project is an example of how the Commission has collaborated with the major utilities to develop cutting-edge research programs. The CES-21 project is also an example of how programs must be tailored to maximize ratepayer benefits.

PG&E, SDG&E, and Southern California Edison started California Energy Systems for the 21st Century (CES-21) through a cooperative research development proposal in 2011. The three major utilities wanted to partner with Lawrence Livermore National Laboratory (LLNL), Idaho National Laboratory, and New Context[45] in a project focused on modeling and simulation of threat and response narrative and to create physical test bed sites to evaluate the impacts of cyber threats on substation equipment. The utilities' goal was to take advantage of LLNL's supercomputing power and New Context's knowledge of cyber threat intelligence and automation.[46] Despite their size and resources, the utilities do not have LLNL's modeling capabilities.

The CPUC approved of the partnership in 2012. (Decision Order 12-12-031.)[47] In the Order, the Commission authorized $152.19 million over five years on CES-21 research activities related to Gas Operations, Electric Operations, Electric Resource Planning, and Cyber

40 Pacific Gas & Electric, Smart Grid Annual Report (2012) https://www.pge.com/myhome/edusafety/systemworks/electric/smartgridbenefits/AnnualReport.pdf.
41 *Id.* at 43.
42 *Id.* at 59.
43 *Supra* note 15 at iv.
44 *Supra* note 40 at 50-51.
45 Business Wire, New Context to Share the Stage with California Utilities and National Laboratories at DistribuTECH Conference & Exhibition in New Orleans LA (Feb. 5, 2019).
46 *Id.*
47 California Public Utility Commission, Energy Research, Development & Deployment (2019) http://www.cpuc.ca.gov/general.aspx?id=4801.

Security.[48] The roll out was not smooth. Immediately following the Order, the California legislature and consumer protection groups reacted to the high price tag placed on ratepayers as well as the CPUC Chief's close ties with LLNL prior to project approval.[49] On September 26, 2013 California Governor Jerry Brown signed Senate Bill 96 into law, amending the Public Utility Code to cut the CES-21 project funding to $35 million over five years and limited the scope to renewable grid integration and cybersecurity.[50] As a result, the CPUC reopened Order 12-12-31, but emphasized it was only doing so to reevaluate "implementation" issues and would not revisit the "foundational broad policy and legal issues related to D 12-12-31."[51] This was an alleviating response from the CPUC, while the bill still stung reopening the decision could have destroyed CES-21 as ratepayer advocates could once again challenge the CPUC's jurisdiction to approve CES-21 and the project's benefits to ratepayers.

The CES-21 project had a five-year timeline, launching in 2014 and concluding in 2019. The post-Senate Bill 96 amended goals of CES-21 are "to improve the cybersecurity of our electric system and integrate emerging renewable technologies into the grid." The cybersecurity goals are accomplished through the project's main focus on machine to machine automation.[52] The Machine to Machine Automated Threat Response (MMATR) is intended to remove the human element from threat response by the creation of a "threat-aware grid architecture capable of making real-time decisions to increase its survivability and resiliency."[53] Automation's additional benefits include reducing outages, minimizing power grid disruption impacts, and improving recovery times and would apply to SCADA systems, generation, transmission, and distribution.[54] To test automated threat identification, the partners focused on three DHS standards of communication techniques: Structured Threat Information Expression (STIX), which "includes adversary activity and contextual threat information that provides a better understanding of a cyber adversary's motivations, capabilities and activities, and supports effective analysis of cyber threat information;" the Trusted Automated Exchange of Indicator Information (TAXII), which "allows automated cyber threat information to be shared across organizations to detect, prevent and mitigate cyber threats," part of the joint utilities' goal of identifying new threats; and Cyber Observable eXpression (CybOX), a "structured language for observable cyber events." [55]

48 California Public Utility Commission, Decision Order 12-12-031 (2012) http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M041/K694/41694931.PDF.

49 The Utilities Reform Network, CPUC Pres Peevey is Judge and Jury for his own Pet Project (December 19, 2012) http://www.turn.org/in-the-news/peevey-judge-and-jury-for-pet-project/.

50 California Senate Bill (SB) 96, Chapter 356, Statutes of 2013. SB 96 includes Sections (§§) 44 and 45 and added § 740.5 to the California Pub. Util. Code http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0051-0100/sb_96_bill_20130926_chaptered.html.

51 *Supra* note at 3.

52 Automation is thought to be necessary by many because of the speed at which an attack can occur and the need to act quickly, but concern over "taking humans out of the loop" has curtailed its development in the project; the partnership is researching it but leaving it out of the scope of production-level systems. Lawrence Livermore National Laboratory, California Energy Systems for the 21st Century 2016 Annual Report (2017) https://e-reports-ext.llnl.gov/pdf/878504.pdf.

53 Joint Utilities Advice Letter to California Public Utilities Commission (Nov. 14, 2014) https://www.pge.com/nots/rates/tariffs/tm2/pdf/ELEC_4402-E.pdf.

54 The National Interest, How California Is Protecting Its Critical Infrastructure from Cyber Threats (Nov. 10, 2016).

55 *Id.*

In 2016, the project moved into physical test phases with a Modeling and Simulation Platform to test utility configurations and attack scenarios, a Physical Test Bed to sandbox on actual equipment, and an Automated Response Research Package covering high-impact risk scenarios to California IOUs, an open-source Indicator Remediation Language (IRL) to allow cross communication and support STIX, a SCADA Security Protocol to protect the SCADA system including a Threat Attribute Scoring Model that assists in quantifying the threat that a particular exploit or malware may pose, for use during Exploit, Malware & Vulnerability (EMV) analysis, simulate threat situations for islanding and attacks from multiple sources, [56] and systems to communicate and detect specific threats. [57] When finished, the CES-21 partners intend to deliver "a research package to lay the foundations for automated threat response and new ways of securing utility communications, and specific platforms for the IOUs to test vulnerabilities and remediations." [58]

The Commission and the utilities have also worked to publicly share the results of the research. On September 27, 2018 via Resolution E-4943, the CPUC authorized the CES-21 partners to open source four software applications.[59] The four applications were industrial control system communications projects "ready to be transitioned from the R&D stage to the next development stage, where they can be used in practical applications [by other utilities]."[60] Under California law, a public utility can request an advice letter from the Commission for approval to transfer an interest in utility property valued at less than $5,000,000.[61] This legal pathway enabled the utilities to quickly and efficiently make the technology available for public license. The utilities submitted, and the Commission, agreed that publicly licensing the technology would produce grid reliability, resiliency, and safety benefits for ratepayers.[62]

The sensitive nature of the information captured and tested in CES-21 has created another issue for the Commission, the difficulty of assessing the outcomes of the project. Due to the presence of confidential information, most of the project outputs and inputs are classified and inaccessible to the Commission and its staff without security clearances. The security clearances are a necessary component of protect confidential information. However, without direct access to the information, Commissioners and Staff are put in a knowledge deficit and must assess outcomes without being able to see the whole picture. Balancing the benefits of protecting data, sharing information with regulators, or releasing information to the public is a tricky issue that California is grappling with and other states may eventually confront.

56 California Public Utilities Commission, 2017 California Public Utilities Commission Annual AB-1338 Report to the Legislature on Trusts and Entities (2018).

57 Lawrence Livermore National Laboratory, California Energy Systems for the 21st Century 2016 Annual Report (2017).

58 *Id.* at 9.

59 California Public Utilities Commission, Resolution E-4943 (2018) http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M230/K600/230600679.PDF.

60 *Id.* at 3.

61 California Public Utility Code, Div. 1 Part 1 Ch. 4 Article 6 §851.

62 *Supra* note 59.

CONNECTICUT

Connecticut's path to cybersecurity action demonstrates how a governor, legislature, and commission can work together with the state's utilities to craft a program. It is also an example of the value of how each level of government must be ready to take advantage of the right conditions. A meeting between a regulator with security expertise and a governor created the traction to move Connecticut's cybersecurity strategy forward. Art House, who was appointed as Public Utilities Regulatory Agency (PURA) Commissioner in 2011 and became PURA Chairman in 2012, was seated beside Governor Daniel Malloy. They engaged in a conversation about Commission priorities and Commissioner House listed cybersecurity as a looming vulnerability. What emerged from that conversation was a series of legislative, gubernatorial, and Commission actions to address grid security. On February 19, 2013, the Connecticut General Assembly adopted the State's Comprehensive Energy Strategy which elevated grid security as a priority and assigned regulatory responsibilities.[63] Foremost, the strategy recognized physical and cyber grid security as a priority for the electricity sector strategy.[64] Second, the Connecticut Department of Energy and Environmental Protection (DEEP) directed the PURA to assess the state's utilities (water, electricity, and natural gas) capability to deter interruption of service.[65]

Utility participation in the cybersecurity assessment was a critical factor in the development of Connecticut's plan. Chairman House wanted to involve the utilities in the process, as well as gauge an honest understanding of the state of the utilities' cybersecurity posture.[66] A strategy was drafted and shared with the participating utilities before being finalized to give the utilities the opportunity to comment.[67] PURA then presented the Governor and General Assembly a report on recommendations to improve deterrence. PURA published the unclassified report April 14, 2014.[68] The Governor invited utility representatives to the press conference announcing the strategy as means of lending political clout to the action plan that followed.[69] On April 6, 2016, PURA published the Connecticut Public Utilities Cybersecurity Action Plan (Action Plan).[70] When developing the Action Plan, participating utilities were given the option to use a usual adjudicatory proceeding style, or to collaborate informally for the change to affect the outcome of the Action Plan.[71] The utilities agreed to meet annually with a representative from PURA and the Division of Emergency Management and Homeland Security.[72] The utilities are expected to report on their cyber defense programs, registered attacks on their systems, and corrective measures they will undertake in the following year.[73] The utilities chose a DHS style Cybersecurity Capability Maturity Model (C2M2) reporting style.[74] The utilities prefer

63 The Connecticut Department of Energy and Environmental Protection, 2013 Connecticut Comprehensive Energy Strategy (2013) https://www.ct.gov/deep/lib/deep/energy/cep/2013_ces_final.pdf.
64 *Id.* at at 100-101.
65 *Id.* at 111.
66 Interview with Art House, Connecticut Chief Cyber Security Risk Officer (November 20, 2018).
67 *Id.*
68 Connecticut Public Utilities Regulatory Agency, Cyber Security and Connecticut's Public Utilities (2014) https://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.
69 *Supra* note 66.
70 Connecticut Public Utilities Regulatory Agency, Connecticut Public Utilities Cybersecurity Action Plan, Dkt. No. 14-05-12 (2016) https://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.
71 *Supra* note 66.
72 *Supra* note 70 at 2.
73 *Supra* note 70 at 2.
74 *Supra* note 8.

this method to enhance communication over legislation, executive order, or regulatory mandate.[75]

The caveat to the informal style was that utilities would still be expected to provide significant details on their current practices. However, to protect this information, the content of the meetings would be confidential, note-taking would be limited, and that information included in the annual report curated to reduce utility exposure.[76] By creating procedures for limiting the exposure of shared information, the utilities and the state were able to focus on the same goal of securing the grid.[77] The next step Connecticut may take is to restructure its cybersecurity management throughout the state.[78] Currently Connecticut uses a "federated cybersecurity management structure" but it does not appear to be optimizing the use of available technical resources, and thus the state may switch to a more "centrally accountable approach."[79]

Connecticut focused on threats to grid operation and did not evolve its program out of a data security initiative. The 2013 Comprehensive Energy Strategy's cybersecurity focus is on protection from the "emerging threat to the electric grid and other elements of the state's critical infrastructure."[80] The overall theme throughout the 2013 report, to the 2014 strategy, to the 2016 action plan, and the 2018 annual report is a concern of a disruption to the grid from a cyberattack, rather than a loss of consumer data. By coordinating the actions of multiple parties, Connecticut was able to rapidly establish and activate a process for information sharing between utilities and PURA while safeguarding sensitive data.

MICHIGAN

The executive branch has a large formal role in Michigan's cybersecurity defense, both in the private and public sectors. After his election in 2010, Governor Rick Snyder, made it his prerogative to prepare Michigan for cyber and physical attacks against critical infrastructure in the state. Additionally, Snyder stressed the criminal element that increased information sharing brings. Warning that "this information ecosystem has created a new avenue for crime, misconduct and espionage," Snyder's additional concern was the potential positive and negative impacts on the Michigan economy.[81] Snyder wanted take advantage of Michigan's high-tech sector and police and defenses forces to protect the state while simultaneously positioning the state as a leader for other states to look to on cybersecurity guidance.

From 2011 through 2015, Governor Snyder laid the foundation of the state's cyber initiative. The executive developed tools for business and industry as well as public sector to respond to cyber-attacks and tasked the Department of Technology Management and Budget

75 *Supra* note 70 at 3.
76 *Supra* note 66.
77 *Supra* note 66.
78 Connecticut 2018 Cybersecurity Update, Executive Summary (2019) https://portal.ct.gov/-/media/Office-of-the-Governor/Press-Room/20180918-Connecticut-Cybersecurity-Annual-Report.pdf?la=en at 4.
79 *Id.* at 4.
80 *Supra* note 63 at iv.
81 Michigan Cyber Initiative, Defense and Development for Michigan Citizens, Businesses and Industry (2011) https://www.michigan.gov/documents/cybersecurity/MichiganCyberInitiative2011_365631_7.pdf at 3.

(DTMB) with developing a "strategic information technology (IT) plan" for the state.[82] The goal was to provide a "framework to assist critical infrastructure owners and operators in the development of a collaborative, public/private team to respond to cyber disruption events affecting the State of Michigan."[83] Additionally, Snyder formed the Michigan Agency for Energy (MAE).[84] The Agency serves as the central energy policymaker in the state and works with the MPSC to develop emergency response plans unique to a cyber-attack.[85]

Information sharing and open dialogue are central features of how Michigan organizes its cybersecurity defense. The executive department meets with the private sector in both formal and informal meetings. Specifically, the Governor meets with private industry to discuss cyber concerns quarterly in through the Cyber Advisory Council and the CIO of the DTMB hosts "CIO Kitchen Cabinets" to bring together CIOs of various industry across the state to discuss mitigation and risk assessment strategies and concerns.[86] Similar to the strategy employed in Connecticut, the use of informal meetings, as opposed to strictly formal, has shown to efficiently flesh out the issues and strategies through the meetings candidness.[87] Finally, the state incorporates the Michigan State Police and national guard into its cyberattack response planning and prevention. For example, the DTMB works directly with the state police to use the MIOC, a 24-hour information sharing system to communicate with state, federal, and private partners. This collaboration ensures up to date information sharing in times of crisis.[88]

The Michigan Public Service Commission (MPSC) plays a complementary role to the executive branch, specifically supporting critical state energy infrastructure. The MPSC believes protection from cybersecurity threats to be part of the Commission's duty to ratepayers.[89] Cybersecurity planning is housed in the Smart Grid section of the MSPC, a subsection of the Operations and Wholesale markets.[90] The Commission's first direct foray into cybersecurity occurred in April 2007, with Case No. U-15278, when the MPSC ordered Staff, regulated distribution companies, and other interested parties to participate in a Smart Grid Infrastructure Collaborative.[91] In December 2011, the MPSC published the results of the U-15278 collaboration, "The Smart Grid Collaborative Report to the Michigan Public Service Commission (MPSC)." The Report included working group discussions on cost recovery, assessing costs and benefits, and customer protection.[92] The following year, the MPSC opened Case No. U-17000 to look into vulnerabilities to the security of the grid posed

82 National Association of State Energy Officials, State Energy Cybersecurity Models Analysis: Michigan Cybersecurity Structures and Programs Profile (2015) https://www.naseo.org/Data/Sites/1/michigan-cyber-profile-12-29-15-final-draft.pdf at 9.

83 Michigan Department of Technology, Management, and Budget, Michigan Cyber Disruption Response Strategy, Protecting Michigan's Critical Infrastructure and Systems (2013) at 1.

84 *Supra* note 82 at 20.

85 *Supra* note 82 at 21.

86 *Supra* note 82 at 19.

87 *Supra* note 82 at 20.

88 *Supra* note 82 at 19.

89 Michigan Public Service Commission, Case No. U-18203 (2016) https://mi-psc.force.com/sfc/servlet.shepherd/version/download/068t0000001UVVQAA4 at 3.

90 *Supra* note 82 at 18.

91 Michigan Public Service Commission, Case No. U-15278 (2007) https://w2.lara.state.mi.us/ADMS/Mpsc/ViewCommissionOrderDocument/7876.

92 Michigan Public Service Commission, The Smart Grid Collaborative Report to the Michigan Public Service Commission (2012).

by the new deployment of Advanced Metering Infrastructure (AMI) and in particular the increase in attack surfaces presented by the Internet of Things (IOT).[93] In November 2016, the MPSC found the issue of "sufficient complexity and importance to merit" opening a cybersecurity docket.[94]

In 2014 during rate proceedings, the MPSC instructed the two largest IOUs in the state Consumers Energy[95] and DTE Electric[96] to provide MPSC Staff with annual reports addressing the utilities' cybersecurity programs and attack prevention.[97] Following this move, the MPSC opened cases U-18043 and U-18203 to address statewide annual reporting. From these cases, in 2018 the Commission updated the Technical Standards for Electric Service, Mich Admin Rule 460.3101 to require annual written or oral reports from all IOUs and electric co-ops.[98] The reports must include details on cybersecurity operations and management, as well as an "overview of major investments in cybersecurity during the previous calendar year and plans and rationale for major investments in cybersecurity anticipated for the next calendar year."[99]

Conclusion

The states profiled in this section are a small selection of states addressing cybersecurity vulnerabilities, but they hold important lessons for starting a distribution system cybersecurity program. Let the structure of the program match the size of the challenge. A comprehensive cybersecurity program comes from a long-term commitment of human and financial resources. Cybersecurity programs can originate from a focused interest or evolve out of other programs like grid modernization. Cybersecurity programs often initiate in the agency with the expertise or resources before spreading out to other agencies. Using available resources is the first and best option, but states should be willing to expand agency jurisdiction or create new agencies as needed. Multiple agencies within the state government can play roles in enhancing system security and responsiveness. Whether an agency leads or follows matters less than if the agency participates and contributes. Lastly, there is no single pathway to improving a state's cybersecurity posture and states should seek the pathway that most efficiently deploys resources while meeting identified objectives.

93 *Supra* note 89.

94 *Supra* note 89.

95 Michigan Public Service Commission, Case No. U-17735 (2014) https://mi-psc.force.com/s/case/500t0000008efsYAAQ/in-the-matter-of-the-application-of-consumers-energy-company-for-authority-to-increase-its-rates-for-the-generation-and-distribution-of-electricity-and-for-other-relief.

96 Michigan Public Service Commission, Case No U-17767 (2014) https://mi-psc.force.com/s/case/500t0000008eft4AAA/in-the-matter-of-the-application-of-dte-electric-company-for-authority-to-increase-its-rates-amend-its-rate-schedules-and-rules-governing-the-distribution-and-supply-of-electric-energy-and-for-miscellaneous-accounting-authority.

97 Michigan Public Service Commission, Issue Brief: Cybersecurity (2018).

98 Michigan Public Service Commission, Technical Standards for Electric Service, (2018) https://dmbinternet.state.mi.us/DMB/ORRDocs/ORR/1768_2017-091LR_orr-draft.pdf.

99 *Id.* at Rule 460.3205(1)(b) (2018).

SECTION 4

FACILITATING ACCESS TO CRITICAL INFRASTRUCTURE CONFIDENTIAL INFORMATION

Key Takeaways

- **The Essential Nature of Information Exchange.** Utilities possess an information advantage on how they are addressing cybersecurity vulnerabilities. A mechanism for exchanging information between utilities and regulators is foundational to building an environment of trust and action.
- **All Information Exchanges Provide Value, Some Provide More.** Commissions should use their power to increase information flow. Annual compliance filings, annual meetings, quarterly audits, and bi-annual audits elevate the base level of knowledge of the regulators and increase confidence in investment proposals.
- **Information Exchanges Must be Structured to Protect Confidential Information.** Utilities and utility commissions should deploy different strategies to reduce the releases of confidential information. Site audits by commission staff reduce the number of documents subject to freedom of information act requests. In-camera meetings without note-taking facilitate open discussions. Critical Infrastructure Confidential Information statutes provide legal protection against the release of sensitive information.

Protecting Confidential Information

Information is the lifeblood of utility sector programs, on that statement there is a consensus. Whether it is information collected by the utility, information collected by government agencies, information shared between the government and the utility, or information shared between the utility and the regulator, information flows drive decision making. Another industry consensus that the current information sharing practices are hampering is the response to emerging cybersecurity threats. Current information sharing practices limit regulator engagement at a critical time for the grid. NARUC identified the need for processes that inform state regulators about cybersecurity, that assist regulators

in developing engagement, and that foster dialogue with utilities and other stakeholders.[100] Access to information can reduce the information imbalance that exists between utilities and their regulators and lay the foundation for more productive discussions on when and where to invest in upgrading the security of the grid.

The information sharing problem exist because utilities hold an information advantage over utility commissions. Information is unequally concentrated, and the parties have different levels of sophistication. Utilities are the source of the data upon which decisions to invest are made. Utilities are tasked with ensuring the security of their business enterprise and utility operations processes and they defend against the daily attacks on their system's security systems. Additionally, large utility holding companies with operations in more than one state can centralize portions of their operations, particularly cybersecurity, which allows them to share their concentrated expertise with their various distribution utilities.[101] Also, utilities with NERC compliance obligations are also transferring best practices to their non-federal regulated utilities. In comparison, the development of expertise and institutional knowledge is a more difficult task for regulators. Regulators have a diverse portfolio of areas that require their attention and resources. Commission staff must be multi-disciplinary, wearing the correct hat at the time it is needed before switching to other tasks.

The mechanics of how to share and review information about utility security plans without creating new vulnerabilities was a consistent concern raised in our interviews and confirmed by our research. The concerns split into two different areas: ensuring compliance with state disclosure or "sunshine" laws and ensuring that data collected by regulators did not become a target for hackers. The source of the concerns is the value of information about the physical and cybersecurity protections of utility infrastructure, utility operations procedures and grid technology. If the information is valuable to the utility and its regulators in identifying and addressing vulnerabilities, then the information is valuable to threats seeking to exploit unprotected areas and disrupt grid functions. Unlocking the first while avoiding the second has created a paralysis about how to share information and what to do with the information.

Information Sharing Through Utility Audits

The value of a robust audit process is demonstrated in the penalty imposed upon Duke Energy for violations of its NERC CIP obligations. In levying a fine a of $10 million, NERC cited a "lack of management engagement, support, and accountability" at the utility that created a serious risk to the reliability and security of the bulk power system.[102]

Consistent audits of utility practices are a way to increase commission understanding of utility operations and they can be structured to avoid creating new vulnerabilities. Audits can be used to ensure that the utilities are developing, updating, assessing, and enforcing internal cybersecurity processes. Audits have the additional benefit of increasing the

100 NARUC, Cybersecurity: A Primer for State Utility Regulators, Version 3.0 (2017).

101 For example, see Duke Energy's Cyber Security Operations Center, National Grid's Cyber 1 Program, and AEP's Cybersecurity Intelligence and Response Center.

102 Blake Sobczak and Peter Behr, Duke agreed to pay record fine for lax security – sources. E&E News, February 1, 2019 https://www.eenews.net/stories/1060119265.

level of regular contact between commission staff and the utilities. Audits can also be used to initiate a discussion of best management practices between the utility and the commission or between utilities. The form and function of an audit can be tailored to facilitate information sharing and enhanced system protection without creating excessive compliance burdens for the utilities. Using audits of both procedure and substance to supplement reporting requirements elevates the overall protection of the system. The level of rigor of the audit should be flexible in recognition of the financial and staffing resources available to commissions.

The following are summaries of different state commission audit procedures of distribution utility cyber and physical security programs. The audits differ in their approaches to protecting confidential information and are reflective of available resources and commission priorities. Some states opt not to collect any confidential information or to require that the utility discuss the details of their programs. Other states require a minimum level of information sharing that can be compiled into a report, while engaging in discussions that are not captured in a publicly released report. Some audits happen on a regular schedule – quarterly, annually, bi-annually – while other audits occur when scheduled by Commission staff. The key takeaway is that there are a variety of options available to commissions and that the best option is one that maximizes information flow while minimizing the creation of new vulnerabilities. What option is best is also a reflection of what resources are available to the Commission now and over the long-term. Audits require financial and human resources to complete, resources that must come from limited budgets and available staffing resources.

FLORIDA

Flexibility in when to perform an audit conserves human and financial resources in the Commission while maintaining institutional knowledge. The Florida Public Service Commission's Office of Auditing and Performance Analysis is a key player in efforts to improve knowledge of the physical and cyber protection of Florida's distribution utilities. Flexibility in analytical methods allows the Commission to adapt to evolving threats by directing review of utility practices with the highest risk profiles. The Office of Auditing and Performance Analysis has completed two reviews of distribution system physical and cyber protections of the four largest investor-owned utilities.[103] In 2014, the Office conducted a review of and published a report focusing on the physical security measures protecting the transmission and distribution substations and control centers of the four IOUS.[104] Cybersecurity was a key component of the 2014 review, but the attention given to the issue was ramped up in the Office's 2018 audit in response to changing threat conditions.[105] The Commission is committed to performing additional audits, but has reserved the authority to determine the timing and the content of the audits. The commitment to performing additional audits strengthens the connection between utility and utility regulator while conserving resources.

103 Duke Energy Florida LLC, Florida Power & Light LLC, Gulf Power Company, and Tampa Electric Company.

104 The Florida Public Service Commission Office of Auditing and Performance Analysis, Review of Physical Security Protection of Utility Substations and Control Centers, December 2014 at 1 (audit directly addressed the Metcalf substation attack).

105 The Florida Public Service Commission Office of Auditing and Performance Analysis, Review of Cyber and Physical Security Protection of Utility Substations and Control Centers, April 2018 (audit directly addressed the Ukraine distribution system cyberattacks).

Managing confidential information access has been a key element of the audit process. Florida's sunshine laws created an additional layer of complexity for the staff and utilities working on the audits. Sunshine laws require certain proceedings of government agencies to be either open to the public or disclosable upon the request of the public. In Florida that means that there is a basic right of access to most meetings of boards, commissions, and other governing bodies of state and local government agencies.[106] For utilities managing sensitive data about their operations and fearful of giving attackers a roadmap to their vulnerabilities, the risk of having information subject to the Sunshine laws is considerable. To combat the risk, the Commission staff worked to limit the number of physical records that were retained in the Commission's possession and thus subject to a public records request. This was accomplished by moving audit operations out of the Commission and onto utility property. Commission staff visited each of the audited utilities where they were given access to key documents and key personnel. After the Commission staff had completed their review and finished with their interviews, they departed without taking any documents back to the Commission offices.

NEW YORK

The New York Public Service Commission's Office of Utility Security is an example of how a commission can develop and deploy internal expertise in cyber and physical security to create robust audit procedures. Formed in 2003, the Office of Utility Security is an eight-person office that conducts quarterly audits of its regulated utilities and serves as a source of knowledge and expertise on key security issues for the other parts of the Commission.

Auditors from the Office of Utility Security make regular visits to the offices of utilities to audit their security practices. The information under audit remains at the physical offices of the utilities and is not brought back to the PSC offices. Furthermore, the information is not compiled into an annual report. Audits are intended to evaluate the current state of protective efforts and identify areas where the utilities can and could be making additional investments. The audits are performed using Office-derived best management practices that combine NERC CIP standards with other practices to determine where the leading edge of physical and cyber security is. By evolving away from using standards, the Office is intentionally choosing to focus on evaluating continual improvement rather than compliance with fixed standards.

The Office of Utility Security also convenes meetings of the regulated utilities as a means of increasing information flow between the utilities. Utilities are presented with the opportunity to have discussions with the regulators present and without the regulators present. Meetings are also held with non-regulated utilities, as described in Section 5, extending the reach of the Commission's influence and allowing for other entities to share their institutional knowledge. The combination of opportunities is intentional, to maximize sharing of information that could avoid or mitigate the effects of an event between all utilities, regulated or not.

106 Florida Office of the Attorney General, Open Government – The "Sunshine" Law http://myfloridalegal.com/pages.nsf/Main/DC0B20B7DC22B7418525791B006A54E4.

CONNECTICUT

Connecticut's Public Utilities Regulatory Authority (PURA) conducts an annual review of the cybersecurity protections of its regulated gas, water, and electricity utilities. The content and the structure of the review are the product of lengthy consultations between regulators and regulated utilities on how to facilitate information sharing without creating new vulnerabilities. The process adopted reflects industry concerns in managing access to sensitive data and the desire to build a long-term review program that promotes continuous assessment and improvement.

On April 14, 2014, Governor Malloy accompanied by legislative leaders and representatives of Connecticut's public utilities, issued the Public Utilities Regulatory Authority (PURA) strategic plan "Cybersecurity and Connecticut's Public Utilities," which presented a roadmap to strengthen the state's cybersecurity defenses.[107] PURA issued the Strategic Plan following up to the state's 2013 Comprehensive Energy Strategy.[108] Governor Malloy and the legislature directed PURA to review the state's electricity, natural gas, and major water companies and to assess the adequacy of their capabilities to deter interruption of service.[109] The Strategic Plan included a number of questions PURA needed to address, and it opened docket 14-05-12, "PURA Cybersecurity Compliance Standards and Oversight Procedures" to meet with utilities to address those questions.[110] The public utilities indicated a strong preference for achieving such enhanced communication through voluntary collaboration, rather than legislation, executive order, or regulatory mandate.[111] In its search for a reporting framework, PURA considered the NERC CIP, NIST Cybersecurity Framework, DOE ES-C2M2, AWWA Process Control System Security Guidance, and FCC CSRIC IV WG4 Final Report.[112]

On January 15, 2015, PURA met with all public utility sectors, the Office of Consumer Counsel (OCC) and the Attorney General's Office.[113] Afterwards, PURA met individually with Frontier Communications of Connecticut (Frontier); UIL Corporation (UIL) and Eversource Energy (Eversource); Connecticut Water Company, Aquarion Water Company and Valley Water; Frontier, Verizon New York, Inc. (Verizon), AT&T Corporation (AT&T), Cablevision Connecticut (Cablevision), Lightower Fiber Networks I, LLC; Lightower Fiber Networks II, LLC and Fibertech Technologies Networks, L.L.C. (collectively, Lightower), Comcast and Cox Communications (Cox) and New England Cable and Telecommunications Association (NECTA), the National Cable and Telecommunications Association (NCTA) and the United States Telecom Association (USTelecom); and Verizon, Sprint, T-Mobile and AT&T Corporation.[114] At these meetings PURA and utilities discussed management and leadership focus on cybersecurity; promoting cybersecurity culture; external support and expertise; and the Council on CyberSecurity's Critical Security Controls for Effective Cyber Defense (a series of best practices for organizations.)[115]

107 State of Connecticut, Public Utilities Regulatory Authority, Docket No. 14-05-12, Connecticut Public Utilities Cybersecurity Action Plan, April 6, 2016 at 1.

108 State of Connecticut, Public Utilities Regulatory Authority, Docket No. 14-05-12, Request to Establish a New Docket on PURA's Own Motion, May 8, 2014.

109 *Id.*

110 *Id.*

111 *Supra* note 107 at 14.

112 *Supra* note 107 at 9-13.

113 *Supra* note 107 at 13.

114 *Supra* note 107 at 13-14.

115 State of Connecticut, Public Utilities Regulatory Authority, Docket No. 14-05-12, Notice of Technical Meeting, March 5, 2015.

After the meetings, PURA concluded that it would structure a Cybersecurity Oversight Program for each industry.[116] UIL and Eversource supported the annual meetings but were concerned to the amount of parties in attendance, pointing to their lack of knowledge of cybersecurity and the desire to keep company information private.[117] PURA did propose a confidence-building measure: that the participants agree on external messaging for possible release after the meetings, seeking to inform the public while protecting sensitive defenses.[118] UIL and Eversource expressed a preference for using the framework of the U.S. Department of Energy Cybersecurity Capability Maturity Model (DOE ES-C2M2) for reporting and suggested using "heat maps" of their cybersecurity posture as an annual reporting mechanism to convey a general sense of the areas requiring the most attention.[119] The DOE ES-C2M2 "provides a voluntary evaluation process that can be used to measure the maturity of an organization's cybersecurity program relative to industry-recognized best practices and to identify opportunities for improvement … it is intended to facilitate an organization's self-evaluation of the maturity and robustness of its cybersecurity risk management program."[120] Aside from just evaluating utility practices, Connecticut also reviews the program structure to determine its effectiveness in achieving desired goals and outcomes. In its 2018 Cybersecurity Update, Connecticut indicated a need to review the current management structure to allow for optimal use of available technical resources.[121]

The result of the consultations is a report that provides insight into the state of cybersecurity efforts while minimizing potential vulnerabilities created by information sharing. The published report does not link specific actions or events to individual utilities while the in-person consultations provide an opportunity for deeper discussions into the current state of security efforts. By negotiating a balance between information shared and information published, Connecticut assuaged the utilities' concerns and allowed for deeper engagement on substantive issues.

KENTUCKY

In 2016, the Kentucky Public Service Commission as part of its Smart Grid docket created a cybersecurity reporting and information sharing process.[122] The cybersecurity reporting and information sharing process that emerged addresses utility concerns over mandatory reporting requirements and confidential information while creating conditions for enhanced information flow between the utilities, the Commission, and the Attorney General's Office. The regulated utilities – investor-owned utilities, cooperatives, and public power utilities - must develop internal processes addressing cybersecurity; however, in recognition of the sensitive nature of the information contained in the internal documents, the utilities are permitted to keep the processes confidential.[123] Instead of filing the processes with the Commission, the utilities must every two years certify the

116 *Supra* note 107 at 14.
117 *Supra* note 107 at 15.
118 *Supra* note 107 at 15.
119 *Supra* note 107 at 15.
120 *Supra* note 107 at 10.
121 *Supra* note 78 at 4.
122 Kentucky Public Service Commission, In the Matter of: Consideration of the Implementation of Smart Grid and Smart Meter Technologies, Case No. 2012-00428 – Order, April 13, 2016.
123 *Id.* at 29.

development of cybersecurity procedures and make a presentation to the Commission (and the Attorney General should they wish to attend) describing the procedures that the utility has adopted.[124] Utilities are advised, but not required, to develop, update, and enforce a management-approved cybersecurity policy that addresses known and foreseeable risks.[125]

The KPSC also took the opportunity to extend the scope of the utility's cybersecurity policies to address multiple resilience phases. The Commission stated that the policy and any procedures developed should identified elements of the utility's systems that are the highest risk for an attack and integrate that risk assessment with "plans for hazard mitigation, emergency response and recovery, and other relevant continuity of service arrangements."[126] By extending the scope of the cybersecurity policy, the Commission recognized the need to pair efforts to reduce vulnerabilities with plans to respond to an incident.

DELAWARE

The Delaware Public Service Commission requires its regulated utilities to submit an annual report on the state of their cybersecurity programs. Delaware's annual filing requirement emerged from a docket opened by the Public Service Commission to assess whether cybersecurity regulations or guidelines where needed to ensure safe and reliable service for consumers.[127] After evaluating different options, the Commission landed on a filing requirement that provided an annual check-in by the utilities but did not require an annual audit.

The Commission created a list of questions that each regulated Class A utility must annually submit answers for. The Commission reviews that information submitted by the utility and makes the answers to the questions available to the public. The Commission is also tasked with evaluating the sufficiency of the questions and assessing whether the questions needed to be updated to reflected changing needs. The list of questions asks utilities for information on how their cybersecurity plans are reviewed and audited, if vulnerabilities to the system and utility assets are assessed, internal hiring and vetting processes, emergency preparedness, and whether the Commission should create additional cybersecurity guidelines and regulations.[128] The Commission does not receive additional information beyond what is submitted by the utility and what is made available to the public. By limiting the amount of information collected, the Commission can reduce the vulnerability of unauthorized data sharing or loss of control of the data that is in the Commission's possession.

124 *Id.* at 29.
125 *Id.* at 29.
126 *Id.* at 29.
127 Delaware PSC Docket 16-0659, Order No. 8955, In the Matter of the Commissions' Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Investor Owned Electric, Gas and Water, October 18, 2016 at 1.
128 Delaware PSC Docket 16-0659, Order No. 8955, In the Matter of the Commissions' Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Investor Owned Electric, Gas and Water, October 18, 2016 at Exhibit A.

Conclusion

State commissions have a range of options for increasing information flow between themselves and utilities. The guiding parameters in the development of the process should be flexibility and continuous engagement. A flexible design allows for a state to match the audit or review process with available short-term and long-term resources. The success of the audit process will in part be determined by strength of efforts to protect confidential information. The level of utility participation and engagement depends on assurances that the process will not create new vulnerabilities. Executing that assurance can be accomplished either through informal or formal methods to managing how data is collected and stored. Audits and meetings do not need to be confined to regulated utilities only, commissions have ways to bring together all utilities. Lastly, the value of an information sharing program multiples as the term of the program grows. Commissions learn more and develop internal expertise and utilities gain trust in the process and the outcomes. And that combination leads to more substantive discussions about how to meet grid security needs.

SECTION 5

ELECTRIC MEMBERSHIP COOPERATIVES AND PUBLIC POWER UTILITIES

Key Takeaways

- **Vulnerable Systems with Resource Constraints.** Electric membership cooperatives and public power utilities are important components of the electric distribution system, with unique characteristics and needs. The human and financial resources available to many of the smaller public power utilities and cooperatives may hinder their ability to identify and address system vulnerabilities. New support and funding mechanisms should be explored.
- **Regulatory Oversight.** Commission jurisdiction over the safety and reliability of cooperative and public power systems is patchwork and not consistently exercised when available.

A POINT OF ACCESS anywhere on the distribution system is a point of vulnerability, no matter who controls the point of access. The level of interconnection between distribution systems means that without defense-in-depth and defense-in-breadth comprehensive security programs, that a system could be compromised from any vulnerability. This simple fact creates pressure to raise the level of protection for every utility, large or small, investor-owned or member-owned. In our research and our interviews, we encountered numerous parties that raised concern about whether cooperative and public power utilities were keeping up with new threats and addressing existing vulnerabilities. The entities raised the issue because of a concern about how the vulnerability of their systems could be affected by the cybersecurity posture of other utilities.

This section examines factors affecting the investment decisions of, the quality and quantity of resources available to, and the regulatory oversight of the safety and reliability of cooperatives and public power utilities.

The Important Role of Cooperatives and Public Power Utilities

The importance of electric membership cooperatives and public power utilities in grid security and resilience efforts is easily demonstrated by the numbers. The scope and nature of cooperatives and public power utilities makes them targets for cyberattacks and an area of pressing concern for protective measures. More than 900 cooperatives operate in 47 states providing electric service to 56% of the nation's landmass.[129] Electric cooperatives provide service to almost 13% of the nation's meters, ensuring the more than 42 million individual customers and 19 million businesses, homes, schools, and other establishments receive electricity.[130] Every years, cooperatives deliver 11% of the total kilowatt-hours sold in the United States.[131] Rural electric cooperatives own and maintain 42% of the U.S. electric distribution lines.[132] More than 2,000 public power utilities provide service in 49 states and 5 territories, serving 15% of all electricity customers.[133] Electric cooperatives and public power entities are significant portions of the bulk electric system: generation and transmission cooperatives provide 5% of American's electricity[134] while public power utilities contribute 10% of total electricity generation and transmission.[135]

The constraints on resources available to electric cooperatives and public power utilities to address cybersecurity and resilience issues is an area of concern. Resource constraints are particularly acute for smaller sized electric cooperatives and public power utilities. While the largest cooperatives and public power utilities are comparable with the investor owned utilities, smaller cooperatives and public power utilities are a unique subset of distribution utilities. For example, Los Angeles Department of Water and Power and the Long Island Power Authority are two of the largest utilities in the country regardless of classification, with customer bases in excess of 1 million meters.[136] The largest distribution electric cooperative in the United States, Pedernales Electric Cooperative, serves more than 300,000 customers.[137] The smallest public power utilities and cooperatives serve a fraction of the customers of their larger counterparts. The median size of an investor-owned utility is 400,000 customers.[138] The median size of an electric cooperative is 13,000. The median size of a municipal owned utility is 2,000.[139] The median sizes are smaller than the average size, indicating that a few large cooperatives and municipal owned utilities skew the numbers. The average size of an electric cooperative is over 21,000 customers.[140] The average size of

129 NRECA, America's Electric Cooperatives: 2017 Fact Sheet, January 31, 2017 https://www.electric.coop/electric-cooperative-fact-sheet/.
130 *Id.*
131 *Id.*
132 APPA, Stats and Facts, https://www.publicpower.org/public-power/stats-and-facts.
133 *Id.*
134 *Supra* note 129.
135 *Supra* note 132.
136 Los Angeles Department of Water and Power serves more than 1.4 million meters and the Long Island Power Authority serves over 1.1. million customers. APPA, Public Power: 2018 Statistical Report (2018) at 17.
137 Cision PR Newswire, Largest Electricity Co-op in the US Connects Its Biggest Solar Installation to Date – Builder Homesite, Inc. Expects to Offset 80% of Its Electric Costs by Using Solar Power, February 16, 2016 https://www.prnewswire.com/news-releases/largest-electricity-co-op-in-the-us-connects-its-biggest-solar-installation-to-date-300220116.html.
138 *Supra* note 129.
139 *Supra* note 129.
140 *Supra* note 129.

a municipal-owned utility is approximately 11,000 customers.[141] Variation between states and within states can be significant with an electric cooperative having more than 100,000 customers being next to a cooperative with less than 2,000 customers.

The size and the variation in utility size can affect the ability to build institutional capacity and to access available resources. Electric cooperatives and municipal owned utilities may receive information about what needs to be done, but the ability to act depends on the availability of human and financial resources. Investments by smaller utilities may be hindered by the ability to recover costs from a smaller number of ratepayers and by the lack of available resources to assist the utilities in identifying and addressing vulnerabilities.[142] Further complicating the response to growing cyber threats is that distribution system technology can vary greatly between cooperatives in the same state which limits the ability to create standardized approaches to system upgrades and fixes. Some utilities operate with a fully functional SCADA system while other utilities operate their systems with pre-SCADA technology. Bridging the technology gap will require individualized approaches that acknowledge the needs and capacities of each individual utility.

Larger cooperatives and public power utilities are implementing advanced protections and pursuing best practices in governance and operations. The Large Public Power Council is an industry leader in cybersecurity with many of its members making key investments in research, technology, and training.[143] The LPPC is the key player in industry efforts to improve and revamp E-ISAC, a key program for collecting and sharing information on cybersecurity threats.[144] Large utilities are better able to implement and support best management practices like system risk analyses and sharing the results with key members of the executive team. For many smaller resource-constrained and expertise-constrained utilities, a similar risk assessment and transfer of information is significantly harder.

Governance Structure

The unique governance structures of electric cooperatives and municipal-owned utilities was identified as another factor affecting resiliency enhancements. Cooperatives are owned and governed by their members. Municipal-owned utilities answer to elected officials. Historically, the utilities were created to ensure local control over electricity delivery and to provide low cost service. In many cooperative articles of incorporation, there is an express mandate to provide reliable service at the lowest cost. Members of cooperative board of directors are often recruited for their business acumen and comfort with balance sheets. Addressing issues like cyber and physical vulnerabilities may require a level of knowledge and expertise not contained in the governing body. Investing in preventing or reducing the

141 *Supra* note 129.

142 Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat (2014) at 19-21.

143 For example see LPPC President John Di Stasio, United States Senate Committee on Energy and Natural Resources, Hearing to Examine the Evolution of Energy Infrastructure in the United States and How Lessons Learned from the Past Can Inform Future Opportunities (February 8, 2018); and LPPC involvement in efforts to improve E-ISAC, APPA, Industry engagement effort boost public power/E-ISAC relationship, November 29, 2018 https://www.publicpower.org/periodical/article/industry-engagement-effort-boosts-public-powere-isac-relationship.

144 J. Anderson, APPA, NYPA, SRP cyber experts get window into how E-ISAC handles data, February 21, 2018 https://www.publicpower.org/periodical/article/nypa-srp-cyber-experts-get-window-how-e-isac-handles-data.

impact of an event of unknown risk, unknown probability, and unknown consequence can be difficult for an organization with a mandate to limit rate increases for its customers. On the opposing side, we heard from multiple interviewees that the management structure of cooperatives and municipal-owned utilities can enable quicker responses to changing conditions than large utilities. Provided that resources are available to respond, and capabilities are in place within the organization.

The Importance of National Trade Associations and Large Utilities

The response to the resource constraint problem has been one of collective action. National trade organizations, state organization, and large utilities are working to alleviate the resource constraints limiting the capabilities of smaller utilities. The organizations are a source of resources and information for utilities seeking to assist on a variety of issues including cybersecurity and for many utilities are the primary sources of educational resources, training programs for system operators and boards of directors, information sharing, and lobbying services.[145]The section highlights some of the actors and actions being taken to assist smaller cooperatives and municipal owned utilities. The section starts with the efforts of the National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) before concluding with the efforts of few larger utilities to assist their smaller colleagues.

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION POSITION AND PRACTICES

The National Rural Electric Cooperative Association (NRECA) is a membership organization representing the interests of rural coops. NRECA is leading efforts to address cybersecurity concerns by providing training and information for resource-limited cooperatives.

NRECA's engagement in cybersecurity protections and processes spans multiple decades. NRECA is a long-time member of the Critical Information Protection Committee and has contributed to the development of current NERC CIP standards. One of NRECA's top priorities is "protecting the nation's complex, interconnected network of power plants, transmission lines and distribution facilities."[146] The tools that NRECA, its member cooperatives, and industry partners currently use are the DOE's Electricity Sector Cybersecurity Capability Maturity Model, NRECA's Guide to Developing a Cybersecurity and Risk Mitigation Plan and Template, Rural Cooperative Cybersecurity Capabilities Program, Cyber Mutual Assistance Programs, and the development of new technology (Essence, which monitors utility network traffic and flags anomalous activity; and Simba, can process a year's worth of data in less than an hour aiming to reduce time to detect cyber-threats) in collaboration with the DOE, National Laboratories, DOD, research universities, and industry partners.[147]

In 2016, NRECA entered a three-year cooperative agreement with the DOE and was awarded $7.5 million aimed to help co-ops create a culture of cybersecurity with resources, tools,

145 I. Pena, M. Ingram, and M. Martin, NREL, States of Cybersecurity: Electricity Distribution System Discussions (2017) at 28.
146 NRECA, Building Cyber Resiliency Across America's Electric Cooperatives, July 2017, at 1.
147 *Id.* at 1-2.

and trainings tailored to their unique needs.[148] One of the programs developed through this funding was the RC3 Self-Assessment Research Program to help co-ops gain the training, tools, and resources they need to build stronger cybersecurity programs.[149] The RC3 Program has four main areas of focus that include "advancing cyber resiliency and security assessments, onsite vulnerability assessments, extending and integrating technologies, and information sharing.[150] The RC3 program held a series of free cybersecurity summits to its members. However, in 2017, only 152 co-ops (out of over 900) participated in the six summits.[151] In addition, through the RC3 program, NRECA has been working with 36 co-ops in developing a self-assessment tool to help electric co-ops prioritize mitigation actions and develop a cybersecurity action plan.[152] NRECA is also able to offer (through the use of the DOE funds), a RC3 SANS Voucher Program, which is no-cost, online cybersecurity training, for those who participate.[153] Guidebooks and Resources were also developed by the program. These include the RC3 Cybersecurity Guidebook Series that will "provide information pertinent to specific job roles within a cooperative"[154] and the Managed Cybersecurity Service Providers Catalogue, which is in partnership with APPA and PreScouter Inc., and funded by the DOE, to "develop a catalogue of managed security service providers that offer commercial off-the-shelf solutions."[155]

AMERICAN PUBLIC POWER ASSOCIATION POSITION AND PRACTICES

The American Public Power Association (APPA) is the national trade association for public power utilities in the United States. APPA's membership includes approximately 1,400 of the 2,000 public power utilities, more than 100 joint action agencies and state/regional associations, and about 300 "industry partners and vendors, government entities, other types of electric utilities, and students."[156]

APPA has identified that cybersecurity at public power utilities is often scattered across senior management, IT, operations, security, HR, and other functional areas. To improve and develop a cybersecurity program, the APPA suggests that a single individual should manage the "process for cyberintelligence information flow within the organization" in an effort to establish sound protocols and information exchange around cyber.[157] The APPA supports physical security standards at the bulk power system' however, it does not support a federally legislated "one-size-fits-all" mandate on the distribution level. The APPA's position is that distribution system cybersecurity efforts should be focused on voluntary

148 S. Covitz, America's Electric Cooperatives, RC3 Leverages 'Cooperation Among Co-ops' to Confront Cybersecurity Challenges, October 2, 2018 https://www.electric.coop/on-the-issues/reliability-security/.

149 *Id.*

150 NRECA, NRECA's Rural Cooperative Cyber Security Capabilities Program (RC3) - New Programs Aims to Foster Cyber Security Resiliency in America's Electric Cooperatives, February 2017 https://www.cooperative.com/programs-services/bts/Documents/Advisories/Tech_Advisory_RC3_Overview.pdf at 1.

151 *Supra* note 148.

152 NRECA, Rural Cooperative Cybersecurity Capabilities (RC3) Program https://www.cooperative.com/programs-services/bts/rc3/Pages/default.aspx.

153 *Id.*

154 *Id.*

155 Prepared for APPA and NRECA by Prescouter, Managed Cybersecurity Service Providers for Electric Utilities, October 2017 at iv.

156 APPA, Our Members, https://www.publicpower.org/our-members.

157 APPA, Cybersecurity Information - Engagement Plan, November 2017 at 4.

programs developed outside of NERC standard development process due to difference in configuration, size, and ownership of the distribution utilities.[158] Utilities should perform self-assessments, participate in cybersecurity training and scenarios, actively monitor their networks, enroll in the Electricity Information Sharing and Analysis Center (E-ISAC), have a documented plan, have pre-incident outreach, and provide local governments with reporting on threats and incidents without allowing sensitive information to be exposed.[159]

The APPA's long-term commitment to cybersecurity has made it a hub of activity. The APPA has partnered with the Department of Energy, trade associations like the National Governors Association, the FBI, Department of Homeland Security, the FERC, and is a key member of the Electricity Sector Coordinating Council.[160] In 2016, the APPA entered a three-year cooperative agreement with the DOE to help public power utilities become more resilient. The DOE provided the APPA with $7.5 million for this effort known as the Cybersecurity for Energy Delivery Systems (CEDS) Program.[161] The Cybersecurity Technology Assistance Program, which is part of the CEDS program, is aimed to "help public power utilities to find a cybersecurity technology solution, match utilities with providers, and provide partial funding to deploy the technology."[162] Applications were accepted through September 2018 "or while funds last."[163] Eligibility for this program is contingent on the completion of the Public Power Cybersecurity Scorecard and an interview with the program team. The Cybersecurity Scorecard is aimed at getting the members speaking the same language regarding cybersecurity and to assess where their first or next dollars for cybersecurity protections would be most useful. The program will provide financial and technical support in exchange for a report from the participants regarding their experience with the deployment and use of the technology over the course of a year.

The APPA takes a "crawl then walk then run" attitude regarding the CEDS rollout and is following its members lead on identifying what cybersecurity initiatives they need. Year One of the program – the "crawl" stage - was focused on identifying the needs of its member utilities and get a cybersecurity baseline through audits and surveys. In speaking with its member utilities, the APPA learned that a large portion of the utilities need staff training and guidance before implementing monitoring technology. In Year Two – the "walk" stage – the APPA provided onsite vulnerability assessments to its interested members. The onsite assessment integrates "processes and technologies to alert public power utilities of threats to cyber and physical systems."[164] The offerings in Year Three - the "run" stage - is currently being defined by the APPA in collaboration with its member utilities. Disbursement of the available funds has been slower than expected as utilities sought greater levels of assistance to simply assess their current security posture and have been delayed in rolling out proposed upgrades.

APPA is continuing to develop products, tools, and training that are tailored specifically to address the unique needs of its different-sized member utilities. APPA is also in the process

158 APPA, Cybersecurity and Physical Security Issue Brief - Grid Security https://www.publicpower.org/policy/grid-security.
159 *Supra* note 157 at 4.
160 *Supra* note 158.
161 APPA, Cybersecurity for Energy Delivery Systems https://www.publicpower.org/cybersecurity-energy-delivery-systems.
162 APPA, Cybersecurity Technology Assistance Program https://www.publicpower.org/cybersecurity-technology-assistance-program.
163 Id.
164 *Supra* note 161.

of developing training tools, such as the Cyber Security Essentials – A Public Power Primer, which "provides an overview of cyber security concepts and issues affecting public power utilities, including trends and recent incidents" through case studies and cyber-attack protection recommendations and best practices.[165]

Utility cybersecurity pilot programs are eligible for funding through APPA's Demonstration of Energy and Efficiency Developments (DEED) R&D program. Utilities, joint action agencies, and state associations must pay a separate membership fee to join DEED and be eligible for the funding.[166] In 2017, 67% of APPA members were also DEED members.[167] DEED members can receive up to $125,000 in funding for a single R&D project, and in 2017, the program awarded $1.2 million in grants and scholarships for 21 new projects and 23 scholarships, technical projects, and student research grants.[168] The Northern California Power Agency (NCPA) used DEED funding to hire a Cybersecurity Analyst Intern to help plan and develop a cybersecurity incident response toolkit and produce a webinar. The toolkit features "template resources such as an incident response plan; sample exercise agenda; and participant instructional memos."[169] The webinar tested the effectiveness of the toolkit through a tabletop incident response exercise.[170]

LARGE UTILITY ASSISTANCE

Larger cooperatives and public power utilities are also filling in the gaps in cybersecurity protections. The larger utilities, often utilities with federally-regulated transmission systems, identified that their distribution customers lack the knowledge and resources to process and respond to cybersecurity vulnerabilities and threats. In response, the utilities are leveraging their internal resources to extend program offerings to the smaller distribution utilities. Participation is voluntary and the adoption curve varies greatly between utilities and regions.

Regulatory Commission Oversight of Safety and Reliability

The smaller size of cooperatives and public power utilities often reduces the attention given to their cyber and physical security protection. However, the interconnectedness of the grid creates conditions where a point of vulnerability anywhere on the system allows entry into the system but is not determinative of where the system might be attacked. Recent reports indicate that experts believe that grid operation systems have already been penetrated and that attackers are laying dormant as they collect information and expand their access.[171] Several interviewees discussed how the connections in a SCADA system mean that any

165 APPA, Cyber Security Essentials – A Public Power Primer https://ebiz.publicpower.org/APPAEbiz/ProductCatalog/Product.aspx?ID=4909.

166 APPA, DEED R&D Funding https://www.publicpower.org/deed-rd-funding.

167 APPA, Supporting Innovation by Public Power Utilities of All Size at 11.

168 *Id.* at 2.

169 APPA, Replicate this Cybersecurity Toolkit – Learn how to best protect your utility from cyber attacks, based on a successful toolkit created in Northern California https://www.publicpower.org/event/replicate-cybersecurity-toolkit.

170 *Id.*

171 P. Kelly-Detwiler, Forbes, Cybersecurity: The Hackers Are Already Through The Utilities' Doors, So What's Next, December 20, 2018 https://www.forbes.com/sites/peterdetwiler/2018/12/20/cybersecurity-the-hackers-are-already-through-the-utilities-doors-so-whats-next/#76f44952158b.

point of access into the grid operation system, whether it originates on a cooperative, public power, or IOU distribution system, puts the entire system at risk. That is why is it important to take a holistic approach to the regulation of safety and reliability and to examine the role of the regulatory commission.

Regulatory commission oversight of electric cooperatives and municipal-owned utilities varies significantly from state to state. A 2008 report on regulatory oversight of cooperatives identified that 16 states did not regulate cooperatives, 8 states regulated cooperatives for terms or service and financing only, 14 states regulated cooperative rates, and 9 states allowed cooperatives to opt in to state regulation.[172] In some states, like Virginia and Vermont, all distribution utilities including cooperatives and municipal-owned utilities are subject to the full regulatory authority of the utility commission.[173] In other states, like Florida, distribution utilities are partially subject to state regulation in the areas of ratemaking, system planning, or safety and reliability. In other states, like South Carolina,[174] electric cooperatives and municipal-owned utilities are fully exempted from state regulatory commission oversight and thus wholly reliant on internal governance processes.

In our research, we found a variety of jurisdictional authorities over safety and reliability of cooperative and public power utilities and a variety of responses on how to address system-wide resilience. Some large public power utilities and cooperatives are subject to federal regulation and therefore must comply with NERC standards. For distribution utilities, the level of state regulation is patchwork. Some states have no jurisdictional authority and do not exercise any oversight. Some states have jurisdictional authority and fully exercise it. Some states have jurisdictional authority but opt not to exercise it. Some states have no jurisdictional authority but seek opportunities for informal collaboration. The following examples expand on how jurisdictional authority does or does not impede a state's ability to assess the security posture of all distribution utilities.

FLORIDA

In Florida, the Public Service Commission has some degree of regulatory authority over all the utilities and the audits are an exercise of the Commission's existing jurisdiction. For IOUs, the Commission has regulatory authority over all aspects of planning, safety, and ratemaking.[175] For rural electric cooperatives and municipal-owned electric utilities, the Commission has the exclusive jurisdiction to prescribe and enforce safety standards for transmission and distribution facilities.[176]

The Public Service Commission's Office of Auditing and Performance Analysis has completed two reviews of IOU cyber and physical security protections of utility substations

172 NRUCFC, Setting Rates: Best Practices for Electric Cooperatives (Part 3), January 4, 2008 at 3.
173 APPA, State Commission Authority to Regulate Public Power Utility Rates, June 2014 at 73-76.
174 *Id.* at 66-67.
175 FL ST Title XXVII, Ch. 366 §§ 366.04(1) and (6).
176 FL ST Title XXVII, Ch. 366 § 366.04(6).

and control centers.[177] The content and the focus of the reports have evolved in response to changes in the threat matrix. The 2014 report, published shortly after the attack on the Metcalf substation in California, focused on physical security. The 2018 report, published after the 2015 and 2016 cyber attacks on the Ukrainian distribution network, increased the attention given to cyber protections. The PSC auditors and analysts engage with Florida's four large investor-owned utilities (IOUs) – Duke Energy Florida, LLC; Florida Power & Light Company; Gulf Power Company; and Tampa Electric Company –[178] to assess the state of cyber and physical security protections of distribution systems. The review focuses on the four IOUs which combined serve almost 8 million customers.[179]

The four IOUs are a major part of Florida's electric distribution network and should naturally be prioritized for enhanced analysis of their protective measures. However, there are 34 municipal-owned utilities, 18 cooperatives, and one more investor-owned utility that provide electricity to Florida customers.[180] In aggregate, Florida's electric cooperatives serve more than 1 million customers[181] and Florida's municipal-owned utilities serve more than 3 million customers.[182] Expanding the review to consider collective impact of the different utility groups would approach grid security from a system-based viewpoint that reflects what makes a system vulnerable.

ILLINOIS

In Illinois, the Commerce Commission does not have regulatory authority over the state's electric cooperatives and municipal-owned utilities. Under state law, the Commerce Commission's jurisdiction is limited to public utilities with cooperatives and municipal-owned utilities being specifically exempted from Commission reliability reviews.[183] The absence of jurisdiction was flagged by Working Group 3 in the Future of Utility Study as an issue of concern for the Commission and industry stakeholders seeking to understand the security posture of all Illinois' distribution utilities.[184] The Working Group specifically highlighted the vulnerability created by having multiple entities connected to the bulk power system. Entities that are subject to different levels of oversight – some, none, all - exercised by different regulators – commission, municipal government, board of directors. Additionally, while limited budgets and resources of the cooperatives and municipal-owned utilities may be a constraint on action, the lack of information sharing between the entities is as serious a matter.[185]

177 Florida Public Service Commission Office of Auditing and Performance Management, Review of Physical Security Protection of Utility Substations and Control Centers, December 2014; Florida Public Service Commission Office of Auditing and Performance Management, Review of Cyber and Physical Security Protection of Utility Substations and Control Centers, April 2018.

178 Florida has five investor-owned utilities, but Florida Public Utilities Corporation is not included in either the 2014 or 2018 reviews.

179 Duke Energy Florida serves 1.8 million customers, Duke Energy Fast Facts, 2018; Florida Power & Light serves nearly 5 million customers, https://www.fpl.com/about/company-profile.html; Gulf Power serves more than 460,000 customers, https://www.gulfpower.com/about-us/our-company; Tampa Electric Company serves more than 725,000 customers, https://www.tampaelectric.com/company/about/vitalstatistics/.

180 Florida Public Service Commission, Facts & Figures of the Florida Utility Industry (2016) at 1.

181 FECA, http://www.feca.com/.

182 FMEA, Florida Municipal Utility Map, https://www.publicpower.com/florida-municipal-utility-map.

183 83 ILL ADC 411.140. Under Illinois law, electric cooperatives and municipal-owned utilities are not defined as "public utilities" over which the Commerce Commission has regulatory jurisdiction, 220 ILCS 5/3-105(a).

184 *Supra* note 11 at 105.

185 *Supra* note 11 at 105.

NEW YORK

A lack of jurisdictional authority does not need to be a barrier to developing understanding of system-wide resilience and cybersecurity efforts. As described in Section 4, the New York Public Service Commission's Office of Utility Security conducts regular audits and performance of its regulated utilities. The role of the Office in improving the security of the distribution system does not stop there. The Office arranges for information sessions with regulated and non-regulated utilities to create opportunities for the whole sector to discuss emerging issues and best management practices. The Commission is also part of the New York Utility Security Working Group which is a collaboration between the Commission, the New York Independent System Operator, the New York Power Authority, utilities, and other government offices. By combining the collective efforts of organizations working on different elements of grid physical and cybersecurity, the Working Group seeks to advance collaborative practices to secure the grid.

Conclusion

A vulnerability anywhere on the system makes the whole system vulnerable. Therefore, it is imperative that utilities - regardless of their size or governance structure - have access to proper education, resources, and funding for the development and implementation of cyber security best practices. Lack of financial resources and human resources impair utilities' ability to address legacy technology issues and to prepare for the coming digitalization of the grid. These problems can be overcome, but it will take a concerted discussion about how to identify, marshal, and distribute the necessary resources to a diverse set of utilities. It is also imperative that commissions consider the whole system when making decisions about where to focus their review efforts. Regulatory jurisdiction has historically constrained commission oversight of cooperative and public power utility safety and reliability; however, as demonstrated, it does not need to constrain engagement and interaction with non-regulated utilities.

SECTION 6

COST CONSIDERATIONS AND COST RECOVERY MECHANISMS

Key Takeaways

- **A Different Type of Investment.** Addressing cybersecurity and resilience requires continuous, incremental investments. The shorter useful lifespans of cybersecurity investments—software and hardware—and the need for continual investment in upgrades can lead to conflicts over cost recovery mechanisms as the choice of mechanism may create a regulatory lag.
- **Cost Recovery Mechanisms Matter.** The question of how costs are recovered is as important as the question if the costs will be recovered. The decision when to file a proposal can be influenced by which recovery mechanism is employed.
- **Rate Case vs. Single Issue Rider.** General rate cases remain the preferred vehicle for assessing the reasonableness and prudence of investments. Adjustment clauses and deferral accounts are not commonly used as recovery mechanisms for cybersecurity expenses. Single issue riders and other special recovery mechanisms could be used to recover incremental expenditures provided they are designed to prevent transferring risk onto ratepayers.
- **Ratepayer Benefits Control.** Ratepayer benefits must be demonstrated for each investment action. For investments in improved ICS and OT security, the link between benefits and consequences is clear. For investment that mitigate the consequences of an incident and facilitate recovery of critical infrastructure, the ratepayer benefit calculation is more complex and less clear. Resiliency metrics are a key piece of justifying proposed investments in all phases of resiliency.

CYBERSECURITY PROTECTIONS AND SYSTEM RESILIENCY flow from investment in cybersecurity and resiliency. The connection is simple as is the need for additional investment. What is not simple is the process of unlocking and optimizing investment. Finding the optimal level of investment that reduces system vulnerabilities while maximizing benefits for the utility and the ratepayer is a question without an easy answer. Invest too little and there is a risk of not addressing vulnerabilities. Invest too much and ratepayers will incur costs above what is needed. Invest in the wrong area and you can get unaddressed vulnerabilities and costs that do not produce a benefit.

The options for spending funds are immense and the issues of how, when, and where to invest are daunting. The need for new software, new hardware, new personnel, and new training programs is visible across utility types and across the country. This section tackles two questions affecting how and when those needs are met: how to align cost recovery processes with system investment needs and whether standard utility accounting practices should be reviewed for their impact on investment decisions. The section begins with the challenges of investing in protections against an anticipatory threat of unknown consequence. The section concludes with a discussion of how the choice of cost recovery mechanism and expense categorization can influence the decision of when to invest in upgrades and updates. Throughout, recent utility filings are used to illustrate the challenges of finding the right balance of the public interest.

Anticipatory Threats

The need for action on grid resilience and cybersecurity is an acknowledged fact across the utility industry. The constant flow of reports and alerts has the industry on notice that it must act to reduce its exposure and to protect its ability to offer safe and reliable service to its customers. The question of how to act has yet to be fully resolved or even fully discussed.

The ability to invest in cybersecurity and grid resiliency is hampered by multiple factors. First, the U.S. has not suffered a major cyberattack and consequently there is little information available to define the potential scope of damage and the total sum of damages.[186] Second, cybersecurity investments are seeking to protect the grid against a threat of unknown and constantly changing consequence. The current annual cost imposed on the U.S. economy by blackouts is estimated to be between $25 and 100 billion.[187] The economic and health and welfare impacts from a series of small-scale blackouts or a large-scale blackout could dwarf existing costs.[188] However, it is difficult to quantify the potential impacts and that difficulty makes it challenging to develop analyses about potential benefits. Third, the interconnected nature of the grid means that investment by one utility is likely to produce benefits shared by other utilities which may lead to suboptimal

186 U.S. utilities have not provided evidence of a significant cyberattack on American facilities; however, a growing number of utility executives state that an attack is likely in the near future.

187 Executive Office of the President, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages (2013) at 3 (estimated costs range between $25 and $70 billion dollars per year); Department of Energy, Smart Grid: An Introduction (2012) at 5.

188 *Supra* note 13 at 4.

investment levels.[189] Fourth, addressing cybersecurity and resilience requires continuous, incremental investments.[190] The investment needs can lead to conflicts over cost recovery mechanisms as the choice of mechanism can create a regulatory lag.

Utility Cybersecurity Investments

Our research and interviews identified growth in utility investment in cybersecurity combined with a pattern of preferred approaches evaluating and recovering costs. Utilities are addressing cybersecurity vulnerabilities by upgrading and adding software and hardware in addition to boosting internal training programs. For example, utility commissions in Rhode Island and Virginia have recently approved investments in distribution system cybersecurity.[191] Cybersecurity investment estimates are projected to increase in concert with the growing attack surface arising from an increasing digitization of the grid from distributed energy resources to the Internet of Things. Global smart grid cybersecurity investments are expected to nearly double in the next decade which will increase the pressure placed on regulators and utilities to find the optimum method for investing in and recovering the costs of securing the grid.[192]

Regulatory Lag and Cost Recovery Mechanisms

Our research and interviews also identified that regulatory lag for cybersecurity investments is a growing concern. Simply stated, the method of cost recovery will increasingly influence how investments were being made and when they are being filed for approval. As cybersecurity capital needs grow, their influence on the decision when to file a rate case will grow too. The decision when to file and when to invest can be influenced by the availability of special recovery mechanisms. As general rate cases remain the preferred vehicle for assessing the reasonableness and prudence of information and operational technology investments,[193] this is an area ripe for discussion. Furthermore, working through these issues now will allow for alignment of investment decisions with security needs in advance of much larger future investments.

The shorter useful lifespans of cybersecurity technology – software and hardware – and

189 Bipartisan Policy Council, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat (2014) at 19-21.

190 Continuous investment is needed to provide the flexibility necessary to combat an everchanging threat matrix.

191 In Rhode Island, the Rhode Island Public Utilities Commission approved a rate settlement agreement with National Grid that included almost $3 million dollars in Operations and Maintenance funds for electric distribution system cybersecurity and almost $2 million dollars in capital investments in electric distribution system cybersecurity, National Grid Settlement Agreement Docket Nos. 4770 and 4780, June 6, 2018 at 44-46 and National Grid Dockets Nos 4770/4780 Attachment 1 Narragansett Electric and Narragansett Gas Revenue Requirement Settlement Terms Rate Years 1, 2, 3, June 6, 2018 at Attachment 1 page 7 of 9. In Virginia, the Virginia State Corporation Commission fully approved the cyber and physical security elements of Phase 1 of Dominion Energy's electric distribution grid transformation plan, a total investment of $35.2 million dollars over three years, Virginia State Corporation Commission, Final Order No. PUR-2018-00100, Jan. 17, 2019 at 6.

192 Navigant Research, Cybersecurity for the Digital Utility - Transmission Upgrades, Substation Automation, Distribution Automation, Smart Metering, and Smart Grid IT & Analytics: Global Market Analysis and Forecast (2017) https://www.navigantresearch.com/reports/cybersecurity-for-the-digital-utility.

193 *Supra* note 145 at 3. These findings were also supported by our interviews with utility commissions on their methods for evaluating cybersecurity investment proposals.

the need for continual investment in upgrades and updates creates challenges for utilities. The lifespan of typical utility plant investment is significantly longer than the five to seven years associated with a cybersecurity investment. Furthermore, there will be a regular need for new investment. As a result, there is a requirement for more flexible regulatory approaches which allow for more regular and immediate recovery of costs. Timing between the filing and approval of rate cases results in regulatory lag which may delay or discourage approval of investments. Cybersecurity protective measures must respond to an everchanging matrix of known threats and prioritized vulnerabilities and the need for timely and certain methods for the recovery of cybersecurity investments is essential.

The Difficulty of How to Recover Costs

How to recover the costs of technology investments is an issue that has generated significant amounts of debate without ever concluding on the best methodology for balancing investment needs and risk allocation. An example from Michigan highlights key elements of the debate over cost recovery that remain unresolved today. In 2011, the Michigan Smart Grid Collaborative ("Collaborative") published a report to the Michigan Public Service Commission. The purpose of the Collaborative was to assist in the development of a strategic plan to guide Smart Grid Deployment.[194] One Collaborative working group focused on cost recovery for smart grid investments and many of the key findings are relevant to the discussion of cybersecurity investment recovery.

The Collaborative report covered the unique nature of information and operational technology investments, difficulties in risk and benefit allocation, and whether non-traditional cost recovery mechanisms were necessary. Information and operational technology investments are unlike traditional utility investments for several reasons. There is a higher level of risk because of the uncertainty over how the technology will function over time.[195] When deploying technology to address an anticipated problem, there is less predictability for the benefits that will be produced. Traditional investments have known benefit profiles that are realized shortly after installation, e.g. reduced congestion, increased capacity, and increased reliability. [196] Technology investments do not have the same predictability which raises the level of risk assumed by the customer or the utility. Furthermore, allocating benefits is harder as there is less clarity in whether benefits are being accrued by the customer, utility, or society. Without safeguards in place, risk can accumulate upon customers.[197]

The Collaborative report discussed the use of non-traditional rate recovery mechanisms, riders and surcharges, but it could not reach a consensus on their value in assisting the deployment of smart grid technologies. The Collaborative could not see a value beyond that offered by a prudency review in a general rate case in ensuring the risks and benefits were distributed fairly among all parties.[198]

194 Michigan Public Service Commission, Smart Grid Collaborative Report (2011) at 4.
195 *Id.* at 46.
196 *Id.* at 47.
197 *Id.* at 47.
198 *Id.* at 47.

Differing Approaches to Cost Recovery

Different approaches to cost recovery are seen in the Rhode Island and Virginia commission orders. Most investment proposals are evaluated through general rate case proceedings, like National Grid Rhode Island's recently approved cybersecurity investment schedule. The investments are part of National Grid's Cyber 1 program which is a long-term program to enhance the resilience of National Grid's distribution operations.[199] National Grid Rhode Island proposed a series of investments under the umbrella of its Cyber Security and Information Services (IS) Technology Modernization Programs.[200] The initial investment proposal covered a wide swath of cybersecurity measures from investments into advanced threat detection technology, communication system encryption technology, and enhanced management capabilities during an attack.[201] On August 24, 2018, the Rhode Island Public Utilities Commission ("RIPUC") approved the Amended Settlement Agreement for National Grid's rate design.[202] Within the plan, the RIPUC approved more than $2 million dollars in direct investment in cybersecurity programs.[203]

Cybersecurity-specific filings like Dominion Energy's electric distribution grid transformation plan are the exception not the rule. In January 2019, the Virginia State Corporation Commission issued its final order on Dominion Energy's proposed plan for electric distribution grid transformation projects. To comply with the Grid Transformation and Security Act of 2018, Dominion proposed a 10-year program to enhance the reliability, resiliency, and security of the electric distribution grid of which the Plan represented the first three years of the program (Phase I).[204] Over the full ten-year term of the program, Dominion requested recovery of $106.9 million dollars of cyber and physical security investments, of which $35.2 million would be recovered in Phase I.[205] The Virginia State Corporation Commission ruled that Dominion's proposed Phase I cyber and physical security investments were reasonable and prudent, but found that the proposed investment in advanced meter technology, emerging technology, customer information platforms, and grid hardening were not, a disallowance of more than $1.3 billion dollars.[206]

The Rhode Island and Virginia examples highlight the different options available for the deployment of special recovery mechanisms. In supporting its requested revenue requirement, National Grid pinpointed the importance of using the appropriate cost recovery mechanism. The company's testimony posed the question: "Why is it important for the Company to obtain cost recovery of the post-Test Year changes to annual rent

199 National Grid Rhode Island, Investigation as to the Propriety of Proposed Tariff Changes, Book 7 of 17, Dockets Nos. 4770.4780, November 17, 2017 at 15.

200 National Grid Rhode Island, Investigation as to the Propriety of Proposed Tariff Changes, Compliance Filing, Book 1 of 7, Dockets Nos. 4770.4780, August 16, 2018 at 43.

201 National Grid Rhode Island, Investigation as to the Propriety of Proposed Tariff Changes, Book 7 of 17, Dockets Nos. 4770.4780, November 27, 2017 at 67-73.

202 Robert Walton, Rhode Island Approves National Grid Modernization Plan, Rate Increase, Utility Dive, (August 27, 2018) https://www.utilitydive.com/news/rhode-island-approves-national-grid-modernization-plan-rate-increase/530924/

203 Rhode Island Public Utilities Commission, National Grid Amended Settlement Agreement, Dockets Nos. 4770.4780, August 20, 2016 at 123.

204 Dominion Energy, Petition for Approval, Case No. PUR-2018-00100, July 24, 2018.

205 Virginia State Corporation Commission, Final Order No. PUR-2018-00100, Jan. 17, 2019 at 6.

206 *Id.* at at 6.

expense for IS projects?"[207] The company asserted that inclusion of the post-Test Year change in Information System rent expense associated with the post-Test Year Service Company Information System investments is necessary to prevent a substantial shortfall in its rate recovery.[208]

In Virginia, utilities seeking approval of an electric distribution grid transformation plan can request a special recovery mechanism. Utilities can apply for a rate adjustment clause or a customer credit reinvestment offset, both options that allow for recovery outside of a general rate case.[209] The rate adjustment clause allows utilities to recover costs outside of a general rate case immediately upon approval of the plan. The customer credit reinvestment offset recovery mechanism creates a second opportunity for utilities to seek recovery outside of a rate case. If the utility opted not to petition for a rate adjustment clause for investments in its electric distribution grid transformation plan, it can request during its triennial review, to reduce the customer credit to allow for recovery of investments in the plan.[210]

Special Recovery Mechanisms in Use

Distribution investment riders employed in Ohio and Texas demonstrate how utility commissions or legislatures can develop procedures for the incremental recovery of cybersecurity investments. In Ohio, utilities can seek recovery of incremental investments in the distribution infrastructure through the Distribution Investment Rider ("DIR").[211] In Texas, utilities can recover the cost of incremental investments via a Distribution Cost Recover Factor ("DCRF").[212] We acknowledge the contentious nature of single-issue ratemaking and we have presented the history and application of each of the riders for the purpose of furthering discussion on if this is an appropriate cost recovery mechanism to use for incremental cybersecurity investments.

The riders share many elements including legislative origins, filing restrictions, program spending caps, and program time limits while demonstrating that different approaches can be taken to control and manage the impact of the rider. In Ohio, AEP Ohio, relying upon the authority granted in R.C. 4928.143(B)(2)(h) to propose single issue ratemaking, sought and was granted approval from Public Utilities Commission of Ohio for a DIR for the purpose of "facilitating the timely and efficient replacement of aging infrastructure to improve service reliability."[213] In 2010, the Public Utility Commission of Texas approved a proposed

207 *Supra* note 199 at 19.
208 *Supra* note 199 at 19.
209 Va. Code § 56-585.1 A.6 (2018) (rate adjustment mechanism; Va. Code § 56-585.1 A.8.d (2018) (customer credit reinvestment offset).
210 Va. Code § 56-585.1 A.8.d (2018).
211 The Public Utilities Commission of Ohio, AEP Ohio's electric security plan, https://www.puco.ohio.gov/be-informed/consumer-topics/aep-ohio-s-electric-security-plan/.
212 16 TX ADC §25.243 (2011).
213 The Public Utilities Commission of Ohio, In the Matter of the Application of Ohio Power Company for Authority to Establish a Standard Service Offer Pursuant to R.C. 4928.143, in the Form of an Electric Security Plan, Case No. 16-1852-EL-SSO and In the Matter of the Application of Ohio Power Company for Approval of Certain Accounting Authority, Case 16-1853-EL-AAM, April 25, 2018 at 79.

rule for more timely recovery of capital investments in distribution infrastructure.[214] The Commission opted to postpone adopting the rule until the Legislature had the opportunity to weigh in.[215] In 2011, the Texas Legislature amended 16 TX ADC §25.243 to create the Distribution Cost Recovery Factor. The DCRF paralleled existing authority for incremental cost recovery of transmission system investment.

Although the DIR and DCRF share similar constraints on their use, the limitations on the DCRF are imposed by regulation while limitations on the DIR are derived through commission action. DCRF and DIR filings are limited in their frequency. DCRF filings can only occur once per year.[216] The DIR is updated quarterly and proposed DIR rider rates are "automatically approved 60 days after the application is filed, unless the Commission specifically orders otherwise."[217] In Texas, the types of invested capital eligible for inclusion in the DCRF are defined by regulation.[218] Furthermore, the return on equity is determined by when the last rate case was filed. If it was within three years, the return on equity approved in the rate case is applied to the DCRF, if it was longer than 3 years there is a regulatory formula for calculating the return.[219] In Ohio, the Commission sets the amount of revenue that the DIR can collect and it performs an annual review of the DIR for accounting accuracy, prudency, and compliance with program directives.[220] In Texas, the expenses are subject to further scrutiny in the next rate case proceeding.[221] In Ohio, the current DIR will sunset at the end of 2020 unless AEP Ohio files a distribution rate case by June 1, 2020.[222] The current tariff established annual DIR rate caps while permitting over and under collection of revenue to be carried over to the next fiscal year.[223]

Considerations in Deploying Alternative Rate Mechanisms

The use of alternative rate mechanisms to accommodate the unique characteristics of cybersecurity investments raises concerns about ratepayer protections. Whether it is single issue riders, future test-years, or another mechanism, the move away from general rate case proceedings as the vehicle for assessing the prudence of investments raises concerns about the proper allocation of risk between customer and utility. The choice to deploy an alternative rate mechanism should only occur after deliberative debate about ratemaking objectives.

A 2014 NRRI report stated that regulators should at a minimum consider the need for alternative rate mechanisms when "conditions change to cast doubt on the efficacy on existing ratemaking methods."[224] The report expanded that "commissions should

214 Public Utility Commission of Texas, Report to the 82nd Texas Legislature, Scope of Competition in Electric Markets in Texas (2011) at 10.
215 *Id.* at 11.
216 16 TX ADC §25.243(c)(1)(C) (2011).
217 *Supra* note 213 at 80.
218 16 TX ADC §25.243(b)(3) (2011).
219 16 TX ADC §25.243(d)(2) (2011).
220 *Supra* note 213 at 80.
221 16 TX ADC §25.243(f) (2011).
222 *Supra* note 213 at 80.
223 *Supra* note 213 at 80.
224 NRRI, Alternative Rate Mechanisms and Their Compatibility with State Utility Commission Objectives (2014) at 7.

consider the merits of alternative rate mechanisms when market, economic, operating, technological, and other conditions change."[225] The evolving security needs of distribution systems are already affecting the economic, operating, and technological conditions. The automation of grid functions, the growth of distributed resources, and the creation of distribution system platforms are reshaping the technology used to deliver electricity services. The balance between long-life and short-life infrastructure is changing as grid integration increases. Continual investment in short lifespan hardware and software components is required just to maintain system performance and security. In combination, the changing conditions can alter utility investment decisions. The question of how to address this issue is a question without an answer, but for which a process exists to discern the answer.

The selection of an alternative rate mechanism should begin with a discussion of the objectives that the rate mechanism is intended to meet. A discussion of the objectives can only begin when there has been an exchange of unbiased information between the utility and the commission that will assist the commission in understanding the consequences of their decision.[226] Protecting the public interest requires no less. Utilities should be prepared to share information on vulnerability and threat assessments, cybersecurity policies and procedures, and internal performance evaluations. Doing so will alleviate the concern that alternative rate mechanisms are solely advancing utility interests. Commissions should be prepared to request and receive the data.

An alternative rate mechanism does not excuse the need for robust oversight. Commission participation in the design and review of the rate mechanism is critical to ensuring the balance of competing interests. Cybersecurity investments reduce the likelihood of negative consequences, an investment that reduces potential costs to produce a benefit. Commissions may struggle with how to properly measure the benefits of a reduction in potential negative consequences. To have effective oversight, this issue must be addressed through the development, deployment, and widespread adoption of resilience-specific metrics, a topic discussed further in Section 7. The combination of metrics and access to information will enable fulsome evaluations of the objectives and outcomes of the rate mechanism.

Uniform System of Accounts

The second issue identified by our research as potentially impacting investment decisions is whether the methodology for cataloguing different types of investments preordained the method of approved cost recovery. In the course of our research, a question was raised as to the effect of what account a utility expense was placed into and the revenue recovery mechanism attached to that account. As noted earlier, we did not encounter concerns about the ability to recover costs, but we did come across questions about how costs were recovered. In allocating expenses into specific accounts, does that afford the same revenue recovery mechanism to all expenses contained in that account? If so, does the uniform application of a revenue recovery mechanism create regulatory risk for short lifespan information technology and cybersecurity investments? This is a question that we have

225 *Id.* at 12.
226 *Id.* at 28.

flagged that will require additional discussion and investigation. The question does capture that concern that the nature of a utility investment – amortization rates, ability to project specific expenditures – may affect cost recovery options and therefore affect investment decisions. If all regulation is incentive regulation, the way expenses are recorded and recovered should be evaluated for its impact on resiliency goals and objectives.

The Uniform System of Accounts is set of accounting principles used across the electricity sector to standardize electric utility expense accounting. The Uniform System of Accounts creates consistency in the reporting of financial information, reduces administrative burden in the preparation of rate case materials, allows for comparability between different expense classifications, and creates an accounting platform that is understood by lenders, investors, and other stakeholders. FERC regulated electric and gas utilities are required to maintain their books in accordance with the Uniform System of Accounts located in 18 C.F.R. Part 101.[227] Non-FERC jurisdiction utilities can use the Uniform System of Accounts developed by FERC and NARUC and annually revised by FERC.[228]

The Uniform System of Accounts fits with the analysis needs of regulators evaluating whether to permit cost recovery. Utility expenses must be reasonable and prudent. Utility expenses must be known and measurable. To complete these analyses, regulators need information and the Uniform System of Accounts organizes and presents that information.

The Uniform System of Accounts is adaptable and, if warranted, could be adapted to align accounting principles and practices with desired outcomes. State legislatures and regulatory commissions can, and do, amend the Uniform System of Accounts to incorporate state-specific elements. An example of a state that has amended its Uniform System of Accounts is Illinois. Illinois adopted the federal accounting guidelines set forth in 18 C.F.R. Part 101,[229] but with several additions and deletions to adjust to state-specific preferences.[230]

Conclusion

Recovering the costs of cybersecurity investments is an issue fraught with opposing viewpoints. What is clear is that improving cybersecurity posture requires a long-term investment strategy to address technology, staffing, and training needs. Cybersecurity investments differ from traditional utility infrastructure investment. Technology components have a shorter lifespan and a greater risk of redundancy. Investment needs will be continuous to address staffing and training needs. Predicting how funds will be allocated will be difficult as utilities must respond to emerging threats and changing risk profiles.

What is not clear is how to best incentivize investment while protecting ratepayers. Our research identified that the method of recovering costs is an important factor in determining how and when utilities will file investment proposals. In discussing

227 Federal Energy Regulatory Commission, Uniform System of Accounts, February 25, 2019 https://www.ferc.gov/enforcement/acct-matts/usofa.asp.

228 *Id.*

229 83 Ill. Adm. Code. Chapter 1, 415.10 (2014).

230 83 Ill. Adm. Code. Chapter 1, Subchapter B.

and resolving this issue, commissions should move cautiously to gather and evaluate information for mechanism design and implementation. The risk of shifting burdens from utilities and ratepayers demands so, but the risk of regulatory gaps demands a fulsome consideration of the current methods for recovering cost. Balancing those two concerns will affect how utilities deploy resources to secure their systems.

SECTION 7

RESILIENCY METRICS: A MEASUREMENT IN PROGRESS; MEASUREMENTS IN DEVELOPMENT

Key Takeaways

- **Resiliency Metrics and Resiliency Investments.** Resiliency metrics measure grid response and adaptation to low-probability, high-impact events, something reliability metrics do not. Without industry-standard metrics to assess utility resilience, utilities will struggle to justify investments that improve resilience and commissions will struggle to evaluate their prudence.
- **Gap Between Metric Development and Adoption.** Despite numerous public and private research projects proposing various resiliency metrics, industry consensus has not embraced any of them and they are not yet regulatory terms of art.
- **Metrics for All Resiliency Phases.** Individual metrics are needed that can measure the benefits of investments in the robustness, resourcefulness, recovery, and adaptation phases.

RESILIENCE METRICS ARE A CRITICAL COMPONENT in justifying investments in distribution system resilience. Metrics allow utilities to self-assess their operations and gather information to support future investment proposals. Metrics build confidence in utility decision making processes and give regulators a means of identifying where performance expectation are not being met. Metrics allow for the evaluation of the success of an investment in achieving a specified system goal. Metrics should support a feedback process that drives continuous improvement of the security posture of individual utilities and the overall grid.

There is an acknowledged need for industry standard resiliency metrics. Over the last

decade, resilience metrics have been the subject of extensive federal and private research.[231] The research efforts are the product of a growing awareness that current reliability metrics are not sufficient to plan for emerging hazards like cyberattacks and extreme weather events from climate change. The 2017 National Academies of Science report, "Enhancing the Resilience of the Nation's Electricity System" ("NAS Report") asserts that reliability metrics are insufficient in the context of low-probability, high-consequence events because reliability metrics focus on normal operating conditions and price load lost to disruption at a flat rate despite the fact that its cost increases with time. Current reliability metrics such as SAIDI, SAIFI, CAIDI, and CAIFI measure grid operations under relatively normal conditions, and reliability investments seek to reduce the frequency of outages. Reliability metrics do not capture the extra costs and resources incurred by efforts to reduce or avoid large-scale, low frequency, high consequence outages.[232] Resiliency metrics, by contrast, measure grid operations under black sky conditions, and resiliency investments seek to reduce the severity of unexpected outages.

There is also an acknowledged need for adoption and consistent application of resiliency metrics. Industry and government sponsored research continue to refine and define key measurable data points that can be used to assess the resiliency of individual facilities and aggregated systems. However, since metrics are relatively recent, there is a gap between their development through research and their deployment by utilities. The NAS report asserts that more research is needed before consensus is reached on which metrics are essential.[233] The NAS report concludes that resiliency metrics are necessary to understand the value and justify the cost of improvements to grid resiliency.[234] Resiliency metrics research should continue to be a focus for industry stakeholders and should receive additional attention and support.

In our interview process, we asked numerous stakeholders about the use of resiliency metrics in their evaluation of cybersecurity investment proposals. We found that there was no consistent use of resilience metrics by commissions and their staff. In many cases, resiliency metrics were not being utilized at all to evaluate proposed investments and system preparedness. Interestingly, awareness of metrics was not a limiting factor. Most stakeholders were aware of the array of evaluation tools available to them, but unsure of which metrics were best suited to evaluate a utility's security posture and guide investment decisions. One stakeholder said that all the existing metrics need to be mashed together to make a single comprehensive set that can assess governance and security protocols, contain forward-looking and retrospective analyses, and cover all the phases of resiliency. Selecting which metrics to use from the pool of compliance metrics, performance-based metrics, operational security metrics, and governance metrics requires is a resource intensive process. Furthermore, once the metrics are selected, running a metrics program requires management support and adequate resources to be fully effective.[235] For example, EPRI estimated that for a security metrics program that "one full time employee with

231 See Presidential Policy Directive 21 (2013), RAND (2015), Sandia National Laboratories (2015), National Academies of Sciences (2017), and Electric Power Research Institute 2017, discussed below.

232 E. Vugrin, A. Castillo, and C. Silva-Monroy, Sandia National Laboratories, Resilience Metrics for the Electric Power System: A Performance-Based Approach (2017) at 8.

233 National Academy of Sciences, Enhancing the Resilience of the Nation's Electricity System (2017) at 31.

234 *Id.*at 33-34.

235 EPRI, Creating Cyber Security Metrics for the Electricity Sector, Version 2.0 (2016) at 3-4.

additional security or data science duties may only be able to manage 5-10 metrics"[236] while simultaneously compiling a list of more than 45 potential operational metrics.

The Need for Resilience Specific Metrics

Resiliency metrics are needed to assess and justify resiliency investments. Current reliability metrics do not adequately measure preparation for low-frequency, high-consequence events such as cyberattack. There continues to be large gap between the development of resiliency metrics and a consensus among utilities on which are essential and which framework to adopt. Without a common framework for measuring resiliency and its social value, resilience investments may be difficult to justify. Resiliency metrics serve a range of purposes from allowing utilities to self-assess capacity and prioritize needs, establishing a common language for utilities, regulators, and communities with which to discuss utility performance and investment, and allowing for the evaluation of physical, policy, and procedural options for responding to prioritized needs.

The difficulty of finding common metrics is an acknowledged truth in the utility industry and the spark for many concurrent efforts to define what makes a system resilient. In 2012, the National Resources Council noted that more numerical precision is needed to shape resilience metrics into format that is useable and widely accepted.[237] In 2016, NARUC wrote that the current definition of resiliency – robustness, resourcefulness, recovery, and adaptability criteria – lacked the precision necessary to be a regulatory term of art.[238] Consistency in measurement and application is the key to developing metrics that provide value to utilities, regulators, and ratepayers.

As efforts increase in the development of metrics, an important distinction must be accepted, security metrics are not the same as security standards and guidelines. Failure to acknowledge this distinction may produce sub-optimal amounts of improvement. Standards do play a role, but it is an introductory role in the move towards more comprehensive evaluation. Security metrics should identify gaps in program performance and evaluate program improvements.[239] A security metric should drive discussion and analysis of a utility's security posture. Standards are reductionist in nature, providing a common language for discussing threats and vulnerabilities.[240] Standards and guidelines can also focus on compliance and not process improvement, leading utilities and stakeholders to point to compliance as proof of system preparedness. Adherence to standards can limit the adoption of best practices and the capacity to evolve procedures and processes in concert with shifts in risk. As EPRI wrote, "standards-based compliance programs may have input into a set of useful security metrics, but any security metrics will need to be tailored to organizational goals and enterprise risk management practices."[241] For commissions seeking information to allow for the evaluation of investment proposals, the quality of the metric will be as important as the quantity of metrics. The metric must drive decision-making on core issues, not just collect data points.

236 *Id.* at 3-4.
237 National Research Council Disaster Resilience: A National Imperative (2012) at 12.
238 National Association of Regulatory Utility Commissioners, Resilience in Regulated Utilities (2013) at 5.
239 *Supra* note 235 at 2-1.
240 *Supra* note 235 at 2-1.
241 *Supra* note 235 at 2-1.

Current State of Metrics Usage

In the past six years, resiliency metric development has been a major focus of public and private research. In February 2013, President Obama issued Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21), which directed the Secretary of the Department of Homeland Security (DHS) to provide to the President a National Critical Infrastructure Security and Resilience Research and Development Plan ("National CISR R&D Plan").[242] The Directive applies to all critical infrastructures, but calls out energy infrastructure as being uniquely critical due to the enabling functions it provides across all other critical infrastructures. This document defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[243] The Plan "should be issued every 4 years after its initial delivery, with interim updates as needed." [244]

As part of our research we surveyed interview subjects as to the type of metrics that their organization employed. Figure 1 contains a pictorial representation into how the metrics interact with each and how they reinforce each other. The most commonly mentioned metrics were:

NERC CIP

The NERC Critical Infrastructure Protection Reliability Standards (NERC CIP) are 9 standards and 45 requirements for the bulk power system (above 100kV) covering the security of electronic perimeters and the protection of critical cyber assets, as well as personnel and training, security management, and disaster recovery planning.[245] Distribution utilities with generation and transmission assets must comply with NERC standards. NERC standards apply to many large distribution utilities, but not all distribution utilities. NERC's CIP Version 5 (CIP V5), adopted in 2013, significantly bolstered cyber security controls and extended the scope of the systems that were protected under the previous CIP Reliability Standards.[246] Among other things, CIP V5 Standards categorized all Bulk Electric System Cyber Systems using a new methodology based on whether a BES Cyber System has a Low, Medium, or High Impact on the reliable operation of BES. In 2020, CIP-003-7 will go into effect to address some issues identified with NERC treatment of Low Impact Cyber Assets.[247] The new order "improves upon the existing Reliability Standards by: (1) clarifying the obligations pertaining to electronic access control for low impact BES Cyber Systems; (2) adopting mandatory security controls for transient electronic devices

242 The White House, Office of the Press Secretary, Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

243 *Id.*

244 *Id.*

245 Tech Target, NERC CIP (critical infrastructure protection), July 2012, https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection.

246 Federal Energy Regulatory Commission, Docket No. RM13-5-000, Version 5 Critical Infrastructure Protection Reliability Standards, 145 FERC ¶ 61,160, November 22, 2013 at 1-5.

247 Federal Energy Regulatory Commission, Docket No. RM17-11-000; Order No. 843, Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls, 163 FERC ¶ 61,032 at 1.

(e.g., thumb drives, laptop computers, and other portable devices frequently connected to and disconnected from systems) used at low impact BES Cyber Systems; and (3) requiring responsible entities to have a policy for declaring and responding to CIP Exceptional Circumstances related to low impact BES Cyber Systems.

NERC CIP standards were employed by the organizations of multiple interviewees. The standards were used to comply with NERC reporting obligations or as a base for more extensive evaluation. Multiple interviewees noted that the CIP standards were limited because they focused on compliance and not risk-based management practices. Compliance with the standards was not the equivalent of being secure and other tools are needed to evaluate utility performance.[248]

ES-C2M2

The Department of Energy developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0 to support a White House initiative led by the DOE, in partnership with the Department of Homeland Security and in collaboration with private and public-sector experts.[249] A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement.[250] The model is organized into ten domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective—target achievements that support the domain. Within each objective, the practices are ordered by Maturity Indicator Level.[251] C2M2 provides descriptive rather than prescriptive guidance, capturing the current security posture and current capabilities.[252] Model practices tend to be abstract so that they can be interpreted and applied by to the risk profiles of utilities of different sizes, structures, and functions.[253]

Several interview subjects use C2M2 in their organizations or as a tool for evaluating the cybersecurity posture of regulated utilities. C2M2's simplicity allows for utilities to assess their current security posture and understand what actions are needed to advance to the next maturity level. A couple of interviewees remarked that C2M2 was helpful in progressing to more advanced protections, but not in assessing the effectiveness of the action taken.

NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) consists of voluntary standards, guidelines, and best practices to manage cybersecurity-

248 National Association of Regulatory Utility Commissioners, Cybersecurity: Primer for State Regulators, Version 3.0 (2017) at 8.
249 US Department of Energy, Electricity Subsector Cybersecurity Capability Maturity Model, V1.1 (2014) at iii.
250 *Id.* at 7.
251 *Id.* at 11
252 *Id.* at 1.
253 *Id.* at 4.

related risk for critical infrastructure owners and operators.[254] The NIST CSF was developed pursuant to Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, issued in February 2013. Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure.[255] The Framework is designed to be used by multiple industry sectors and is not designed specifically for the electricity sector.

The Framework provides a common taxonomy and mechanism for organizations to assess the current security posture, describe their target security posture, prioritize opportunities for improvement, evaluate progress, and communicate risk to internal and external stakeholders.[256] The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. A Framework Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.[257] The Framework is not designed to replace existing cybersecurity processes and can be overlaid with the existing processes to determine where the organization should prioritize expenditures to manage identified risks.[258] For example, C2M2 scoring can be an input into the CSF analysis.[259]

APPA SCORECARD

In 2018, the APPA released its Public Power Cybersecurity Scorecard, a 14-question self-evaluation based on the C2M2 tool.[260] The tool was developed as part of APPA's three-year cooperative agreement with the DOE to help public power utilities become more resilient. APPA has identified that cybersecurity at public power utilities is often scattered across senior management, IT, operations, security, HR, and other functional areas. To improve and develop a cybersecurity program, the APPA suggests that a single individual should manage the "process for cyberintelligence information flow within the organization" in an effort to establish sound protocols and information exchange around cyber.[261] The Scorecard is part of a larger cybersecurity effort that includes participating in cybersecurity training and scenarios, actively monitoring their networks, enrolling in the Electricity Information Sharing and Analysis Center (E-ISAC), having a documented plan, performing pre-incident outreach, and providing local governments with reporting on threats and

254 National Institute of Standards and Technology, Cybersecurity Framework, https://www.nist.gov/cyberframework.
255 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, (2018) at 1.
256 *Id.* at 2.
257 *Id.* at 3.
258 *Id.* at 13.
259 SGIP's Cybersecurity Committee Framework Implementation Case Study Task Force, NIST Cybersecurity Framework Implementation Case Study (2017) at 27.
260 American Public Power Association, New Cybersecurity Scorecard for Public Power, July 12, 2018 https://www.publicpower.org/publication/new-cybersecurity-scorecard-public-power.
261 American Public Power Association, Cybersecurity Information: Engagement Plan (2017) at 4.

incidents without allowing sensitive information to be exposed.[262]

The Cybersecurity Technology Assistance Program, which is part of the Cybersecurity for Energy Delivery Systems program, aims to "help public power utilities to find a cybersecurity technology solution, match utilities with providers, and provide partial funding to deploy the technology."[263] Applications were accepted through September 2018 "or while funds last."[264] Eligibility for this program is contingent on the completion of the Public Power Cybersecurity Scorecard and an interview with the program team. The program will provide financial and technical support in exchange for a report from the participants regarding their experience with the deployment and use of the technology over the course of a year.

In the course of our research, multiple interviewees identified the Public Power Cybersecurity Scorecard as a good tool for starting the process of evaluating a utility's cybersecurity posture. The Scorecard did not require a large investment of resources to complete and it produced a result that all levels of an organization could understand. However, it was also noted that a utility must have access to other tools and metrics in developing a robust cybersecurity program.

262 *Id.* at 4.
263 *Id.* at 4.
264 *Id.* at 4.

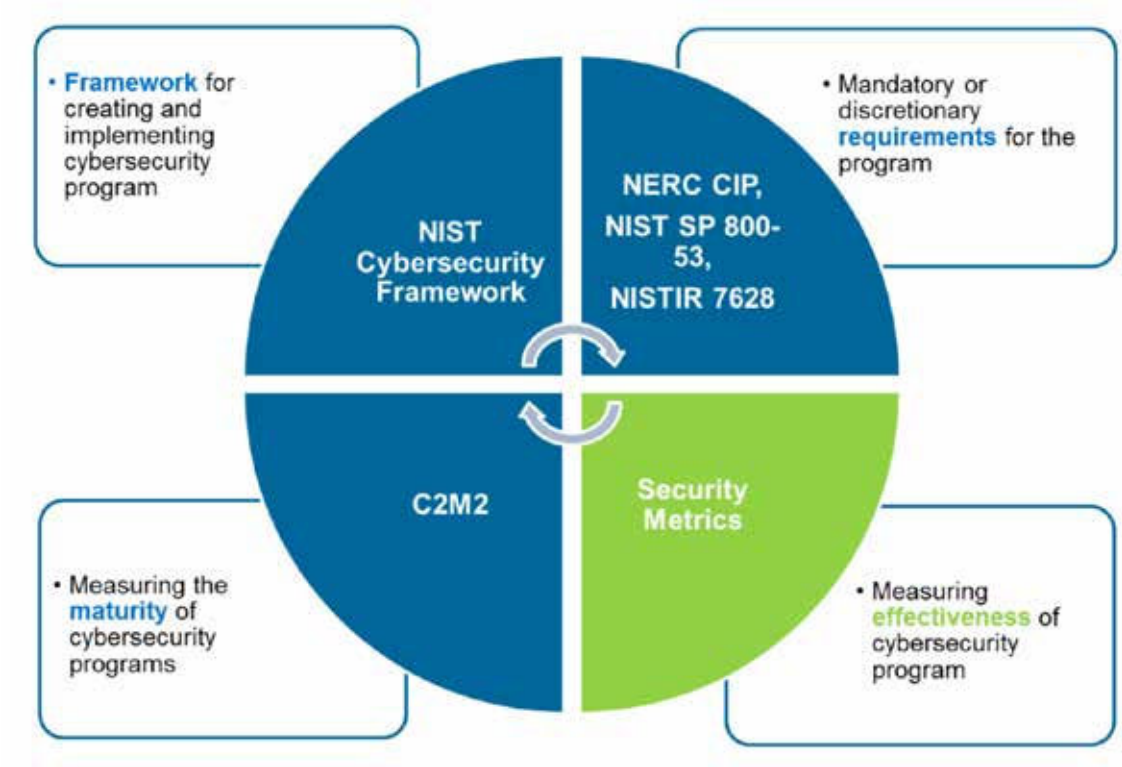


Figure 1: Relationship between metrics[265]

Developing and Adopting Advanced Metrics

Efforts are underway to develop and deploy the more advanced metrics that can identify individual utility resiliency needs and evaluate the performance of existing investments. What are the relevant metrics for achieving the above goals remains a question without a consensus answer. But it is a question that must be answered to give utilities and their regulators a common taxonomy to discuss pathways for securing the grid. This portion of the section discusses why this hurdle is difficult to overcome before profiling advanced efforts to develop and test forward-looking metrics.

DIFFICULTY IN DEVELOPING METRICS

The absence of widely accepted metrics is an acknowledgement of the difficulty of quantifying and qualifying resilience. There is a lack of consistent, quality data on the impacts of a low frequency, high consequence event. Data scientists have no historical data with which they can estimate geographic, temporal, or economic impacts.[266] Nor are there actuarial tables for the impacts of the types of events considered in a resiliency analysis of an anticipatory threat.[267] Modeling the likely impacts and the changes in probability

265 EPRI, Creating Cyber Security Metrics, Volume 3 (2017) at 1-4.

266 U.S. DOE Grid Modernization Laboratory Consortium, Grid Modernization: Metrics Analysis (GMLC1.1) Reference Document, Version 2.1 (2017) at 8.1.

267 *Id.* at iv.

associated with specific protective or responsive measures requires the quantification of multiple unknowns. Additionally, the huge margin of error for each unknown further reduces the value of any modeling effort.[268]

In 2015, the RAND Corporation released a survey of existing resiliency metrics.[269] The RAND report identified 58 papers containing 154 resiliency metrics with most metrics found in the electricity sector and most of the electricity sector metrics being performance based at the facility level.[270] The report notes that resiliency metrics "are used for many purposes and at many levels. Some of the reasons for metrics are more relevant to a federal perspective and others to a local or facility perspective. For example, at a national or regional level, it may be important to know how resilience affects economic output or economic damage stemming from disasters. For a refinery operator, it may be more important to know how many spare parts are in stock and what options exist for backup power generation." The report concludes: "the literature on outcomes of energy system resilience reflects [the goal of making communities safer and more productive] and includes many potential outcome metrics. The literature does not, however, provide clarity about how to adjust capabilities and system performance to most effectively achieve desired outcomes."[271]

Faced with those challenges, research laboratories are rising to meet the challenge. In 2017, Sandia National Laboratories released a report describing and advocating for a resiliency metric framework.[272] The Sandia report describes a seven-step process for establishing resiliency metrics that begins with defining resilience goals, includes determining the extent of disruption and gathering data, and ends with evaluating resilience.[273] Sandia's model is an extension of the Resilience Analysis Process (RAP) model described in the 2015 Quadrennial Energy Review.[274] The model and its extension allow for the customization of metrics for utility or system specific analysis by identifying and estimating the consequences of disruptions to those individual systems.[275]

Later in 2017, the Electrical Power Research Institute (EPRI) issued the third version of its Cyber Security Metrics for the Electric Sector report. The EPRI Cyber Security Metrics project is a three-year project focusing on "on developing, testing, and refining a practical method to quantify the effectiveness of cyber security controls and to accumulate the quantified data over a period of time to provide meaningful, scientific cyber security information to various stakeholders."[276] The EPRI report builds strategic, tactical, and operational metrics from more than 160 data points. The data are drawn from "various points in the utility operations" and "the resulting tiers of data [help] a broad range of utility stakeholders gain improved knowledge about cyber security postures and thus

268 *Id.* at 8.1.
269 This report was used heavily in subsequent Sandia Reports, which said it "should be referenced as a collaborative document." RAND Corporation, Measuring The Resilience of Energy Distribution Systems (2015).
270 H. Willis and K. Loa, RAND Corporation, Measuring The Resilience of Energy Distribution Systems (2015) Fig. 4.2, 4.3 at 12.
271 *Id.* at 24.
272 *Supra* note 232.
273 *Supra* note 232 at 15-26.
274 *Supra* note 232 at 15.
275 *Supra* note 232 at 17
276 *Supra* note 265 at vii.

inform decision-making about policies, investments, and actions plans."[277] The report proposes metrics at several levels of abstraction: "3 strategic level metrics, 10 tactical level metrics, and 47 operational level metrics, for a total of 60 metrics. Each metric is calculated from several related lower-level metrics, forming a hierarchical pyramid-like structure, in which 120-150 data points on the base provide a quantitative foundation. … Operational metrics measure real-time, day-to-day operations such as logs, rule sets, and signatures. Tactical metrics address programmatic health and progress in the organization. Strategic metrics measure corporate risk and alignment of the metrics to the direction of the business."[278]

The EPRI data points and their assembly follows:[279]

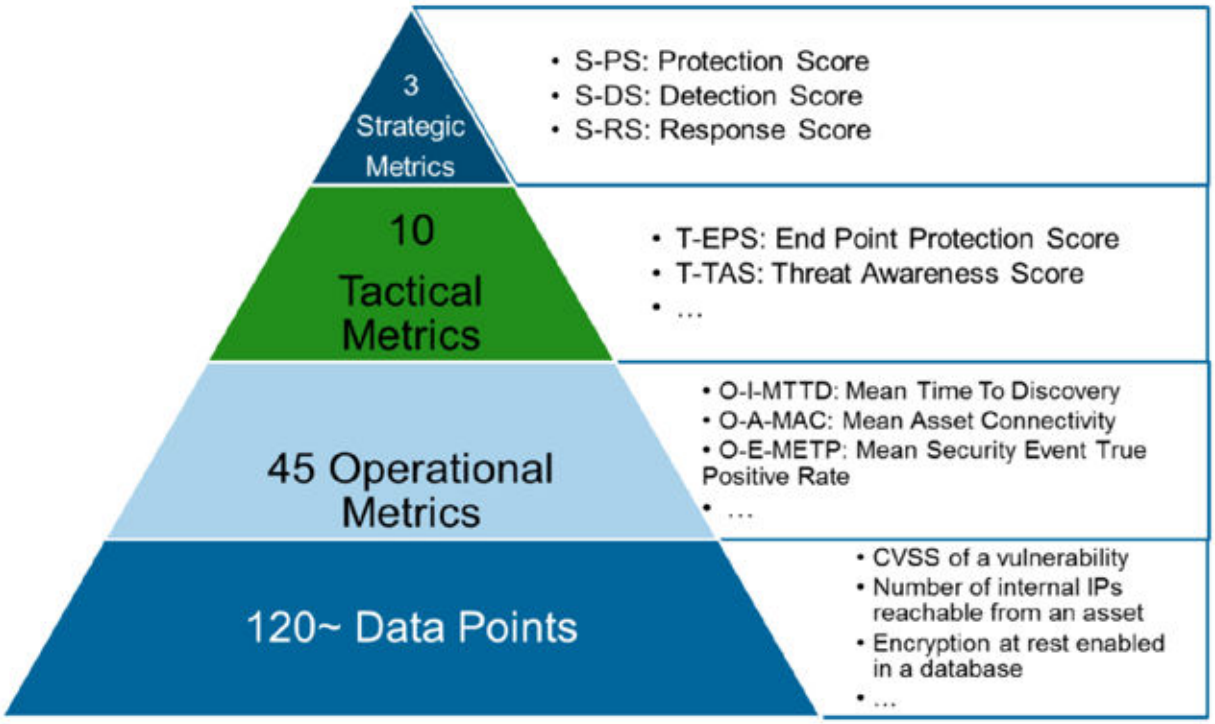


Figure 2: EPRI Metrics Organizational Structure[280]

277 *Supra* note 265 at 1-5.
278 *Supra* note 265 at 1-1; 1-5.
279 Supra note 265 at 1-2, 2-2.
280 *Supra* note 265 at 1-5.

The EPRI and Sandia National Laboratories reports have been the most robust efforts to define resiliency metrics to date. Both highlight the need for context-specific metrics to evaluate current and future investments. Sandia offers a series of steps that can sharpen and hone metrics to provide utility-specific value, a way of sorting through the noise to find out what is important. The EPRI metrics offer quantification of impacts and a method for measuring performance. It is the combination of these types of metrics that could lead to industry-wide accepted metrics that allow for aggregated benchmarking and the evaluation of individual utility performance.

A Role for Commissions

The development of industry resiliency metrics will be a significant step towards reducing the barriers of unfamiliarity and uncertainty that are handicapping utilities and commissions as they seek to make and approve prudent investments. It will not be the last step, widespread adoption and use must follow the creation of the metrics. This is where commissions can and should play a significant role. Commissions should actively explore whether to embrace resiliency metrics in their policy, and how resiliency metrics will improve their evaluative procedures. Utilities should work with commissions to determine which resiliency metrics best measure and improve their cybersecurity posture. Commissions can advocate for industry benchmarking around specific security objectives, e.g. preventing, detecting, mitigating and recovering from events. Commissions can request that their utilities test out metrics that assess their current cybersecurity posture and model the impact of future actions. It is only through use that utilities and regulators will become comfortable with resiliency metrics and what it means to increase the resilience of a system.

Different Phases of Resilience

Since investment decisions are often tied to the ability to demonstrate cost-effectiveness and ratepayer benefits, metrics development should address all phases of resiliency. We draw attention to this issue because how resilience metrics are being developed and how they might be deployed are essential questions that will affect overall system performance and preparedness.

For the purposes of this report, we use the same four resiliency phases as NERC[281] which are:

1. **Robustness** – System operations are optimized to withstand and absorb attacks. Actions taken in this phase focus on responding to information from threat identification and vulnerability assessment efforts.

2. **Resourcefulness** – System operations are optimized to mitigate consequences of an attack. Actions taken in this phase focus on developing systems that can detect and respond to an ongoing event. System segmentation and automated responses are examples of mitigation measures that can limit the consequences and scope of an attack.

281 NERC Reliability Issues Steering Committee, Report on Resilience, November 8, 2018 at 5.

3. **Recovery** – System operations are optimized to return basic services, e.g. critical infrastructure, as soon as possible. A combination of policy, physical, and procedural options can be deployed to identify and prioritize certain sections of the grid.

4. **Adaptability** – After initial services have been restored, the system moves into a recovery period in which stakeholders meet to assess system performance and identify opportunities for improvement. Lessons learned are used in planning for future investments that will minimize the risk of another attack or reduce the consequences of another event.[282]

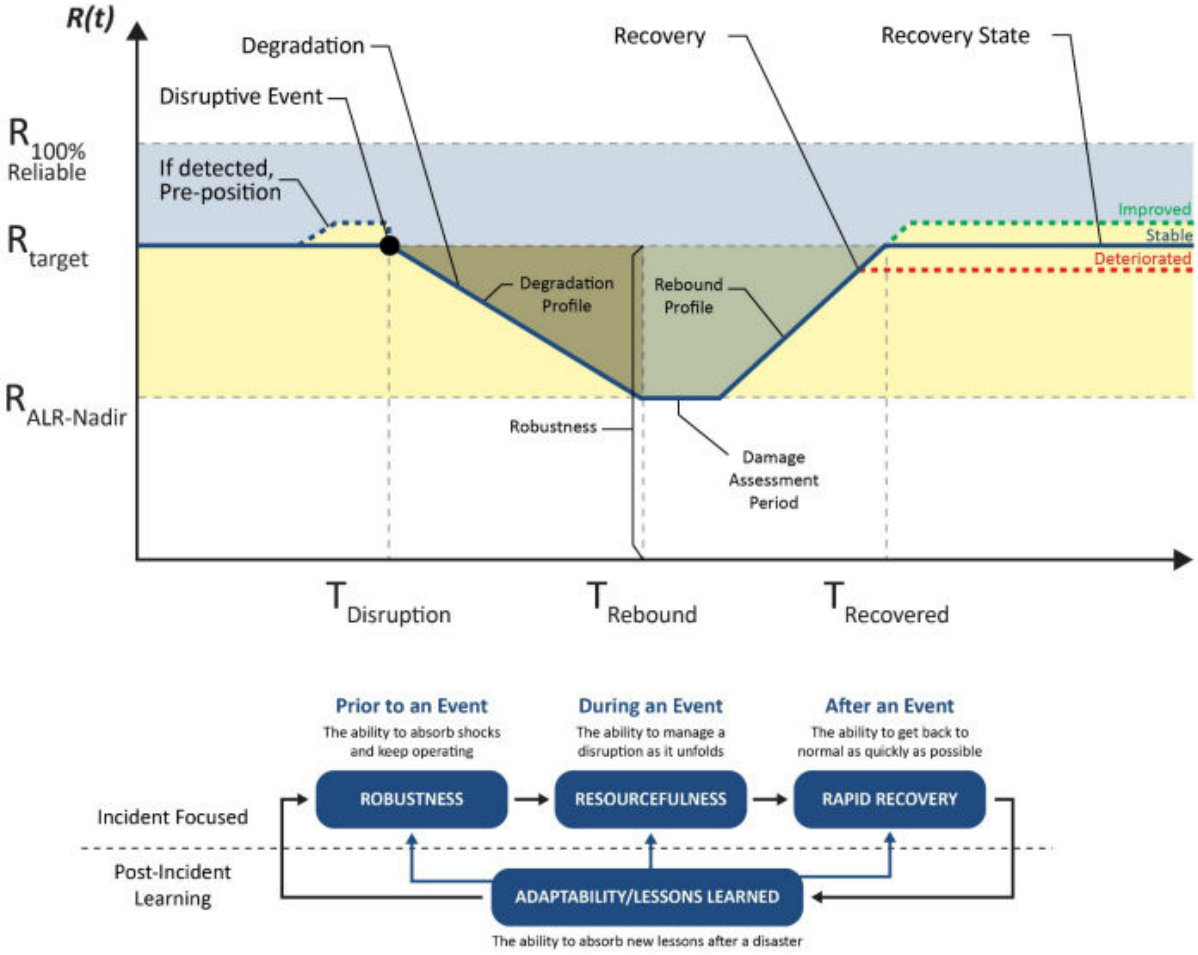


Figure 2.1: RISC's Model for Reliable Operation of the BPS
(from NERC Reliability Issues Steering Committee Report on Resilience, November 2018, p5)[283]

282 B. Unel and A. Levin, Institute for Policy Integrity, Toward Resilience: Defining, Measuring, and Monetizing Resilience in the Electricity System (2018) at 7-8.

283 *Supra* note 281 at 5.

The different phases of resiliency create additional complexity for utility planners and regulators seeking to evaluate investment proposals. But the complexity is not evenly distributed amongst all the phases. Attention is needed to ensure that the uneven complexity does not create an asymmetry in investment patterns that results in an imbalanced response to emerging threats. What makes the uneven complexity? The measurable variables for each phase are different, access to consistent data is inconsistent, modeling of system performance requires different levels of resources, integrating asset-based and performance-based assessments together is complicated, and the lack of real-world data on consequences are some of the reasons why complexity can vary. The effect of the complexity may mean that certain benefits, e.g. system security upgrades, are easier to quantify and allocate than benefits in enhancing the recovery capacity of the system.

A resilient system is resilient across all four phases. Thus, a resilient system requires investment across all four phases. The deployment of resources to enhance the second and third phases, robustness and recovery, is necessary to maintain a system that can mitigate the consequence of an event and speed the return to normal operations. However, the resources that support these phases can be more difficult to secure because of issues in allocating costs and benefits. For example, in several interviews, microgrids were mentioned as a resource that could be used to prioritize protection and operation of critical infrastructure. The inclusion of microgrid investments in a utility's rate base can be a contentious issue as the benefits and costs of a microgrid may be unevenly distributed among ratepayers. Further study into quantifying the resilience benefits of a microgrid may reduce this tension and permit more substantive investment into resources that assist in building out the resourcefulness and recoverability of a system.

Conclusion

The use of metrics to justify and evaluate cybersecurity investments is not currently a common practice. It must become one as commissions begin to grapple with questions about the best way to improve system resiliency. Commissions and utilities have roles to play in advancing metric use and metrics understanding. The most commonly used metrics can provide summary analysis of a utility's security posture, but they do not allow for consistent forward-looking analyses of available options. For a metric to gain widespread adoptions, it must be consistent and repeatable. The metrics must offer utilities and Commissions the ability to evaluate individual performance in unique circumstances while also allowing for system-wide comparisons. Cybersecurity investment needs will grow significantly as the grid digitization and interconnections increase, building knowledge of metrics now will pay dividends later when utilities and commissions deal with the question of what the best path is forward.

SECTION 8
SUMMARY

COMPLICATED PROBLEMS RARELY HAVE SIMPLY SOLUTIONS. Protecting the most complex machine ever invented from a cyberattack was never going to be a single-step process. To protect the distribution grid from the emerging and intensifying threat of cyberattack, we must draw upon existing strengths, reevaluate current practices, and create new tools. This report identified barriers to protecting vulnerable distribution grids and some of the best practices for eliminating those barriers.

Our research and interviews identified multiple areas for action. Improving information flows between regulators and utilities to create an environment of trust and action. Reviewing the activities of all distribution utilities to reduce overall system vulnerabilities. Developing and deploying new financial resources and support programs to empower action in every size and type of utility. Evaluating cost recovery mechanisms to ensure that they are incentivizing the prudent deployment of new technologies and programs. Developing and incorporating resilience metrics into commission and utility practices to improve system function and protect ratepayers.

This report breaks down a complicated problem, how to secure the distribution grid against a cyberattack, into actions and questions. The report provides examples of where action is being taken and who is taking that action. The report captures when there were questions about how to act and who can act. Acting on each of the identified areas and resolving the identified questions will require cooperation and commitment from many stakeholders. Everyone will be involved in protecting our grid. Improving the cybersecurity of the distribution grid will take time, but the time to act is now.

APPENDIX

Interviewees

JENNIFER MURPHY
NARUC, Director of Energy Policy and Senior Counsel

LYNN COSTANTINI
NARUC, Deputy Director - Center for Partnership and Innovation

SHERRY LICHTENBERG
NRRI, Principal, Telecommunications Research and Policy

DANIELLE SASS BYRNETT
NARUC, Director of the Center for Partnerships & Innovation

MATT ACHO
NARUC, Program Officer, Center for Partnerships & Innovation

CARL PECHMAN
NRRI, Director

SUE GANDER
National Governors Association, Director of Center for Best Practices Environment, Energy and Transportation Division

DANIEL LAUF
National Governors Association, Program Director, Center for Best Practices Environment, Energy and Transportation Division

MARGARET BRUNNER
National Governors Association, Senior Policy Analyst, Center for Best Practices, Homeland Security and Public Safety Division

MICHAEL GARCIA
National Governors Association, Senior Policy Analyst, Center for Best Practices, Homeland Security and Public Safety Division

ART HOUSE
State of Connecticut, Chief Cybersecurity Risk Officer

JOHN SENNETT
New York Public Service Commission, Director of Office of Utility Security

BRIDGET WOEBBE
New York Department of Public Service, Assistant Counsel

CARL VINSON
Florida Public Service Commission Office of Auditing and Performance Analysis, Public Utilities Supervisor

PHILIP ELLIS
Florida Public Service Commission Office of Auditing and Performance Analysis, Public Utilities Supervisor

CINDY MILLER
Cindy Miller, LLC; Florida Public Service Commission, retired

CECIL VIVERETTE
Rappahannock Electric Membership Corporation – CEO, retired

CHRIS VAN LOKEREN
North Carolina Electric Membership Corporation, Chief Information Officer

STEVE MYERS
North Carolina Electric Membership Corporation, Field Services Manager

MATT HARTIGAN
Delaware Public Service Commission, Deputy Director

KEVIN NEILSON
Delaware Public Service Commission

ANDREA BRACKETT
Tennessee Valley Authority, Chief Cybersecurity Officer

RANDY CRISSMAN, SR
New York Power Authority, Reliability and Resilience Specialist, Utility Operations

KENNETH CARNES
New York Power Authority, VP Critical Secure Services and Chief Information Security Officer

CHAD HEITMEYER
AEP, Director of Transmission Strategy and Grid Development

BILL ALLEN
AEP, Managing Director, Rate Case Management

AMY MESROBIAN
California Public Utility Commission, Supervisor, Emerging Procurement Strategies, Energy Division

JONATHON LAKEY
California Public Utility Commission, Lead Analyst, Energy R&D Programs

DELIA PATTERSON
American Public Power Association, Senior Vice-President of Advocacy and General Counsel

MICHAEL HYLAND
American Public Power Association, Senior Vice President, Engineering Services

NATHANIEL WEBSTER
American Public Power Association, Senior Director of Electric Reliability Standards and Security

KEVIN WAILES
Lincoln Electric Systems, Administrator & CEO

About Vermont Law School's Institute for Energy and the Environment

Vermont Law School leads the nation in preparing students for the energy transition. Our energy law program has the largest selection of clean energy law and policy courses available, leading clean energy experiential opportunities, and seamless integration with a world class environmental law and policy program, including unparalleled climate law course offerings. The Institute for Energy and the Environment is a national and world energy policy resource focused on the energy policy of the future. The Institute serves as a center for graduate research on the transition to a clean energy future and maintains a vibrant student-staffed energy clinic, which works on legal and business models for community energy development. Students at VLS can pursue a JD in Energy Law, a Masters in Energy Regulation and Law and an LLM in Energy Law.

About the Authors

ADAM MCGOVERN is a 2019 Masters in Energy Regulation and Law candidate.

JUSTIN SOMELOFSKE is a 2020 JD/Masters in Energy Regulation and Law candidate.

CLAIRE VALENTINE-FOSSUM is a 2020 JD/Masters in Energy Regulation and Law candidate.

KRISTEN ZWEIFEL is a 2020 Accelerated JD candidate.

MARK JAMES is an Assistant Professor of Law at Vermont Law School and a Senior Research Fellow at the Institute for Energy and the Environment. He can be reached at: markjames@vermontlaw.edu.

For more information contact:
Institute for Energy and the Environment
Vermont Law School
164 Chelsea St. P.O. Box 96
South Royalton, VT 05068
www.vermontlaw.edu/energy

Institute for Energy and the Environment
VERMONT LAW SCHOOL

VL
VERMONT
LAW SCHOOL