PHASE 2 REPORT

IMPROVING THE CYBERSECURITY OF THE ELECTRIC DISTRIBUTION GRID

Pathways to Enhancing 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 | NOVEMBER 2019

PREPARED BY

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

AUTHORS

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

© 2019

REPORT COMMISSIONED BY PROTECT OUR POWER

PROTECT OUR POWER

www.protectourpower.org

TABLE OF CONTENTS

I PREAMBLE

PROTECT OUR POWER IS AN INDEPENDENT, NON-PARTISAN, NOT-FOR-PROFIT ORGANIZATION, with deep utility industry and electric grid-related experience and insight. Our all-volunteer Advisory Panel includes experts from government, regulatory and emergency response entities, the military, finance, insurance, renewables and academia. Our mission and focus is singular: To make the grid better-prepared to prevent or defend against a major incoming cyber-attack, and to recover from any such attack rapidly.

Protect Our Power recognizes that individual states are critical to upgrading the electric grid —state regulators oversee local electric distribution systems, including reviewing and approving proposed utility investments in grid hardware and software. While the Federal Energy Regulatory Commission oversees the national-level bulk electric system, it is at the state level that "the rubber meets the road" in terms of grid hardening and modernization.

With this in mind, Protect Our Power commissioned Vermont Law School's (VLS) Institute for Energy and the Environment to conduct a two-part study to (1) analyze existing state-level barriers to making grid improvements (Phase 1), and (2) identify potential, practical solutions to overcoming those barriers (Phase 2). Vermont Law School and the Institute have extensive experience working with state utility commissions and, thus, bring to the analysis a high degree of insight and credibility.

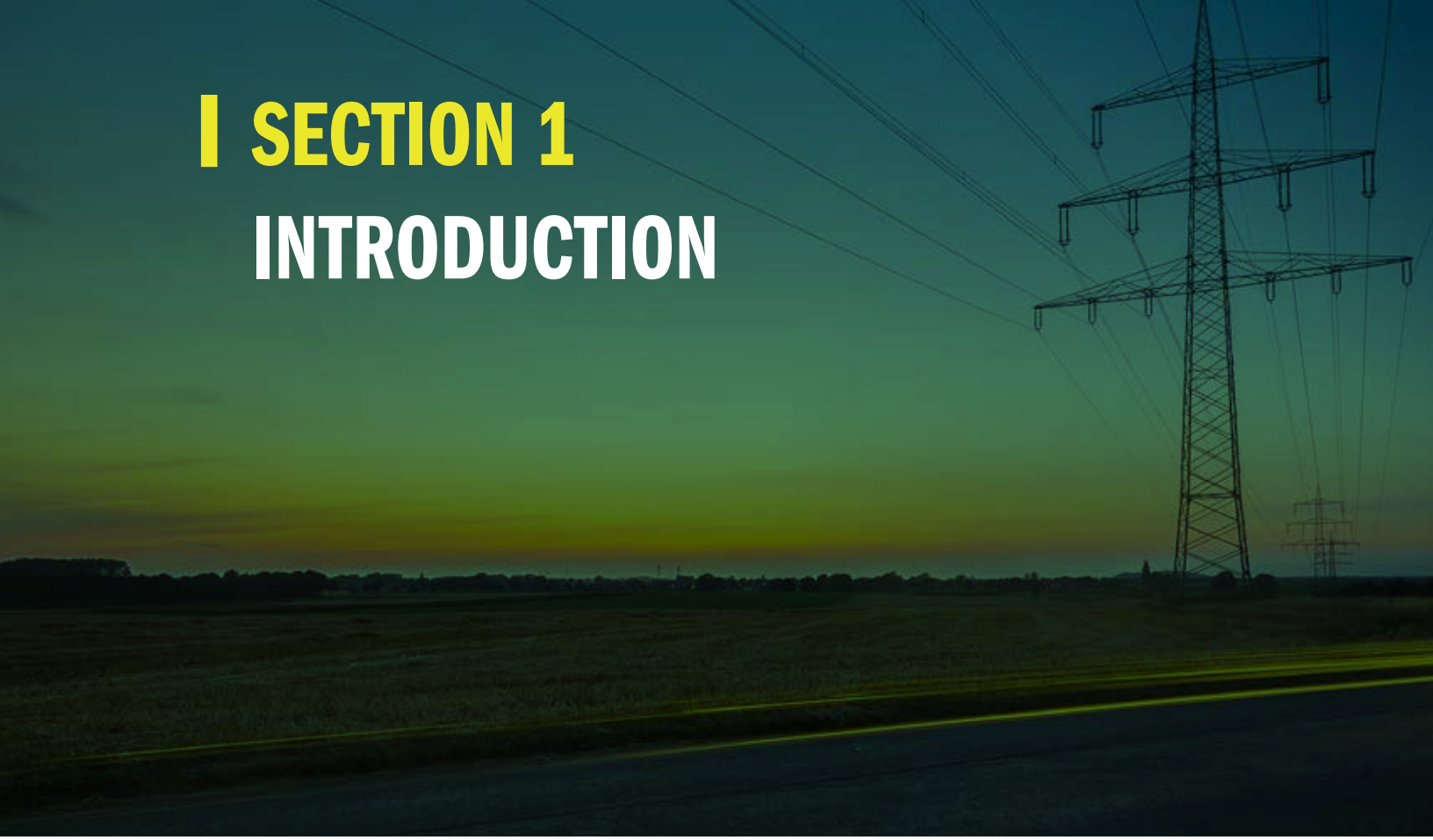
In its Phase 1 report, released in April 2019, the VLS team provided insights, outlined knowledge gaps and identified five specific, overarching barriers to making grid improvements in a timely and effective manner.

In this Phase 2 report, the VLS team defines potential solutions to overcoming those

barriers, and identifies specific ways in which utilities, state regulators, state legislators, governors and federal agencies can work together to implement practical solutions to address critical grid concerns.

Protect Our Power is committed to working with utilities, state and federal officials and agencies, and the U.S. Congress to identify critical challenges to securing our nation's electric grid, to bringing a clear, independent voice to discussions and debates about solutions, and to helping the utility industry succeed in implementing those solutions in the most timely and effective manner achievable. Reliable, affordable electricity is the lifeblood of our economy, our society and our national security, and the time for action on the solutions outlined in this report is now, before an attack cripples or destroys a significant portion of our electric supply system.

For more information on Protect Our Power, please visit: www.protectourpower.org



SECTION 1
INTRODUCTION

OUR ELECTRIC GRID IS AT A KEY POINT IN ITS EVOLUTION. Changes in how we produce and consume energy are reshaping the basic structure of the grid. Automation and digitization are connecting new devices and parties to the grid. What was already the most complicated system in the world is becoming even more complicated. The coming changes offer tremendous benefits, from supporting a zero-carbon economy to establishing a more democratic energy platform. The coming changes in security also foreshadow a future of increased cyberattacks and disruptions to the electricity distribution grid that supports our economy and health and protects our environment.

Our Phase 1 report, released one year ago, identified issues and hurdles that are slowing efforts to enhance cyber preparedness: information asymmetry and a lack of communication between utilities and their regulators; a lack of investment in critical infrastructure; and, a limited understanding of overall system needs. In this Phase 2 report, we tackle how to resolve those issues. The complex nature of each of the issues means that simple solutions are not going to work. What will work are tools that help information move between utilities and regulators, incentivize investment while protecting the public interest, assess system performance and system needs, and ensure that cybersecurity is a fundamental objective of grid modernization plans.

The issues and options presented in this report build upon each other. **Section 2** focuses on protecting confidential information about our critical infrastructure, which is the first step in creating the types of information flow that are necessary to facilitate robust and timely discussions on system needs. **Section 3** presents proactive measures that public utility commissions can take to evaluate and assess the cybersecurity preparedness of their utilities. Cybersecurity investments have a unique profile that requires special cost

recovery considerations. In **Section 4**, guidance on using alternative rate mechanisms to incentivize investment, while protecting the public interest, is provided. **Section 5** discusses how utilities and commissions can work together to develop and implement resiliency metrics. Measuring and improving system resiliency is a complicated task. But the best practices for system operation only arise when utilities and utility commissions know how the system is performing and what the system needs. Examples of making cybersecurity a core objective of grid modernization are discussed in **Section 6**. Across the country, states are opening grid modernization dockets with the goal of getting ahead of the massive changes that are coming. Engineering the new grid with cybersecurity as a core objective will simplify the transition to a more fully integrated energy system.

Each report Section contains multiple examples of how to approach an issue. The diversity of examples indicates that states can take an approach that fits their individual circumstances and available resources. Some states will have existing processes that can be tasked with a new purpose. Some states will have authority that has not been exercised. Other states may need to implement new processes or create new powers for their commission.

The Phase 2 report takes the position that best practices in cybersecurity are preferred over standards. Standards play a role in elevating utility activity to meet a static requirement, but standards do not promote the continuous improvement necessary to manage an ever-evolving threat matrix. Each part of a cybersecurity system must be kept current. Utility best practices promote self-assessment, ongoing education and training programs, continuous outreach and engagement with partners, and a culture of vigilance. The examples presented in the report were chosen because they promote these concepts. The examples also consider how to manage and implement system changes while simultaneously protecting the public interest whether that be access to information or transparency and due process in cost recovery.

This report uses examples drawn from federal statutes, state statutes and regulations, court decisions, and commission orders to highlight potential pathways for action. This method of highlighting is intentional, done to demonstrate that pathways already exist along which action can be taken. The original intent or purpose of a given pathway may differ from what would be asked of it now, or in the future, but that is not a limitation. Utility commission practices have historically evolved to meet new challenges and opportunities.

Grid modernization is happening every day, whether driven by a plan or a threat. The looming question is whether it will be shaped by coordinated effort involving utilities, regulators, stakeholders and legislators working together, or whether it will happen in a unstructured and unguided manner. Grid modernization dockets provide an opportunity for utilities and regulators to proactively build cybersecurity into the next evolution of the grid. Active engagement can create adaptive and flexible processes, able to shift in accordance with available knowledge and current threats, and ensure that critical issues such as confidential information protections and third-party vendors are addressed early and completely. The changing grid will no doubt create new cybersecurity risks, but the time is now to install practices and policies that can confront those challenges.

SECTION 2

CRITICAL INFRASTRUCTURE CONFIDENTIAL INFORMATION

THE MOVEMENT OF CONFIDENTIAL INFORMATION is a critical element in improving the cybersecurity posture of utilities and broadening the institutional capacity of regulators. Information contained in vulnerability and risk assessments helps identify areas of needs and courses of action. System audits assess the performance of existing investments. Meetings between utilities and regulators create a platform for exchanging updates and plotting progress forward.[1] But creating pathways for information to flow must be paired with an awareness of how state disclosure laws may impact efforts to keep information confidential. Just as the information developed and disseminated by these processes is incredibly valuable to system operators and systems regulators, it holds a different value for parties seeking to gain unauthorized access to critical operating systems.

The Phase 1 report presented how the need for more information sharing competes against the need for enhanced information security. Regulators voiced a need for more information to facilitate engagement on key issues and questions. The utility industry expressed concerns that current information sharing practices are hampering the response to emerging cybersecurity threats. Industry concerns split into two related but distinct areas: ensuring compliance with state disclosure or "sunshine" laws and ensuring that data collected by regulators did not become a target for hackers.[2]

State disclosure laws exist to balance the interest of public disclosure against the value of confidentiality. The tension between restricting public access and facilitating public access

1 Vermont Law School, Improving the Cybersecurity of the Electric Distribution Grid, Identifying Obstacles and Presenting Best Practices for Enhanced Grid Security, Phase 1 Report, April 2019 at 21.

2 *Id.* at 22.

exists because access to critical energy infrastructure information can fuel beneficial or detrimental outcomes. The balancing act of determining what information should be made available, who should have access, and under what terms and conditions is a stress point for legislators and regulators.

Clarity in the types of information protected and in the type of protection afforded is necessary to assuage industry fears. Critical infrastructure information protections are common. Since 9/11, more than half of the states have passed public records and public meetings exemptions for critical infrastructure, including private energy infrastructure.[3] Critical energy infrastructure and, in particular, cybersecurity protections are less prevalent, but gaining in their adoption as governments and government agencies grapple with the unique threat of a cyberattack.

Critical infrastructure information protections must evolve to meet the growing threat of a cyberattack. Our research reveals three key steps for managing critical energy/electricity infrastructure information (CEII):

1. Define critical infrastructure within public records law;
2. Exempt critical infrastructure from public meetings laws through formal and informal means; and
3. Balance the public interest in access against the risk of disclosure.

This section highlights examples of statutory language – federal and state – that expand protections to critical infrastructure information while balancing the public's interest in disclosure. The intent of this section is to provide examples of statutory and regulatory language that facilitate information sharing without increasing system vulnerability and to demonstrate how those protections are applied by state utility commissions.

The examples below demonstrate a pattern of evolving protections for critical infrastructure information to meet the risk of a cyber attack. The exemptions crafted by the states are both expansive and focused. The statutory exemptions address the reality that the evolution of the grid is creating new and previously unknown vulnerabilities. The exemptions recognize the connection between utility systems and other critical infrastructure systems and the need to make and protect resilience plans. The changing relationship between the physical and virtual assets that power the grid is captured by some states while others focus on the types of communications that will require protection. In total, the examples present multiple pathways for taking the first step to reducing system vulnerabilities, improving information flows information without increasing risk.

Step 1: Defining Critical Energy/Electricity Infrastructure Information (CEII)

The process of protecting CEII begins with defining CEII so that regulators, utilities, and stakeholders have a shared understanding of what information should be protected and when a public records request should receive heightened scrutiny. This section starts with the federal definitions of CEII because states can and do adopt the federal definitions. The rest of the section presents how states are updating their protections for critical infrastructure information.

3 National Conference of State Legislatures, Open Government Laws and Critical Energy Infrastructure. http://www.ncsl.org/research/energy/open-government-laws-and-critical-energy-infrastructure.aspx#state.

Federal Definitions of Critical Energy/Electricity Infrastructure Information (CEII)[4]

State governments can and are drawing upon the federal government's definition of CEII. The Federal Energy Regulatory Commission (FERC)'s regulations contain definitions for critical energy infrastructure and critical electricity infrastructure. Many states have opted to incorporate or directly reference FERC's definitions within their own CEII laws and regulations.

FERC's definitions contain multiple elements that help critical infrastructure protections deal with cyber threats. First, there is a connection between the source of information and the potential use of information. The definitions identify that the information may be generated by the Commission or received by the Commission. The definition also identifies the purpose for non-disclosure is to thwart an attack on CEII. Second, there is a restriction on exempting all types of details about the infrastructure from possible disclosure, which recognizes the public's need for access to the information. Third, the definition covers physical and virtual systems or system components. In a digitized world, there is no separation between the physical and virtual components of infrastructure. Fourth, the definition identifies who might legally possess the information – Federal, State, political subdivision, or tribal authority. Lastly, there is a connection to the federal National Infrastructure Protection Plan, which allows for updating of definitions and accessing of knowledge of other federal government agencies.[5]

FERC DEFINITIONS

Critical Energy Infrastructure

(2) Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

(i) Relates details about the production, generation, transportation, transmission, or distribution of energy;

(ii) Could be useful to a person in planning an attack on critical infrastructure;

(iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and

(iv) Does not simply give the general location of the critical infrastructure.[6]

4 The terms critical infrastructure, critical energy infrastructure, and critical electricity infrastructure are used in this section as they are presented in different federal and state statutes. The definitions spring from the federal government and are used to draw distinctions between different sources and types of information. This paper uses the more general and all-encompassing "critical infrastructure information" to discuss the types of information shared between utilities and regulators, unless there is a specific term employed within a statute or regulation.

5 Department of Homeland Security, National Infrastructure Protection Plan, https://www.dhs.gov/cisa/national-infrastructure-protection-plan.

6 18 C.F.R. § 388.113(c)(2).

Critical Electric Infrastructure

(3) *Critical electric infrastructure means a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.*[7]

Critical Electric Infrastructure Information

(1) *Critical electric infrastructure information means information related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the Commission or other Federal agency other than classified national security information, that is designated as critical electric infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act. Such term includes information that qualifies as critical energy infrastructure information under the Commission's regulations. Critical Electric Infrastructure Information is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3) and shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records pursuant to section 215A(d)(1)(A) and (B) of the Federal Power Act.*[8]

FERC has also developed regulations for designation and treatment of CEII.[9] Those regulations build off the definitions by creating a common understanding of how the information should be managed, which are valuable in constructing a system that protects CEII while facilitating access.

State Incorporation of Federal Definitions

PENNSYLVANIA

Pennsylvania is an example of a state that aligns its critical infrastructure definition with that the federal government, albeit as a portion of the definition and not the complete definition. Under Pennsylvania law, the government may limit or prevent disclosure of a public record if the record includes:

> *"lists of infrastructure, resources and significant special events, including those defined by the Federal Government in the National Infrastructure Protections, which are deemed critical due to their nature and which results from risk analysis; threat assessments; consequence assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments ... ."*[10]

7 18 C.F.R. § 388.113(c)(3).
8 18 C.F.R. § 388.113(c)(1).
9 16 U.S.C. § 8240-1(d)(2)(A).
10 Pa. Cons. Stat. 65 § 67.708(b).

ALABAMA

Alabama explicitly links its definitions of critical infrastructure and critical energy infrastructure to those promulgated by the federal government. Under Alabama law, any citizen has the right to inspect and make copies of any public writing of the state, unless otherwise expressly provided by the state. However, the following records are exempted from disclosure:

> *records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined at 42 U.S.C. § 5195c(e) as amended) and critical energy infrastructure information (as defined at 18 C.F.R. § 388.113(c)(1) as amended) ....*[11]

State Definitions

State definitions for critical infrastructure vary in their focus and their detail. Definitions can expand what is critical infrastructure beyond energy infrastructure and often are intended to connect with the state's emergency preparedness and response duties. In the wake of 9/11, more than half of the states passed public records and public meetings exemptions for critical infrastructure, including private energy infrastructure.[12] Those exemptions tend to focus on protecting data that could be used in a terrorist attack, which as the example below demonstrates can cause unexpected issues.

Recently, states have passed specific public records and public meetings exemptions for cybersecurity CEII, recognizing that past provisions may not be robust enough to protect against modern threats. States have developed or modified the statutory definition of CEII to reflect changing threats and threat actors. Other states have, as noted above, aligned their definitions with the federal definition of CEII. In any of the cases, a clear and comprehensive definition is necessary to cover the unique system vulnerabilities that a threat vector would seek to exploit and to avoid potential confusion over what information is covered by the protection. The following case study from Washington demonstrates the value of a precise, clear definition of what are exemptible materials.

Terrorism Definition

States often define what information should be protected within the context of how that information might create a risk. Post 9/11, many states implemented definitions that focused on whether the disclosure of information could increase the risk of a terrorist attack. For example, Delaware and Indiana are states that reference terrorism in the public records laws.13 In 2002, Delaware updated its Freedom of Information Act in response to the terrorist attacks of 9/11.14 The state amended the Act to include exemptions from public records disclosures for documents that could "[f]acilitate the planning of a terrorist attack,"

11 Ala. Code § 36-12-40.

12 *Supra* note 3.

13 Delaware's terrorist attack condition can be found at Del. Code Ann. tit. 29 § 10002(1)(17); Indiana's terrorism risk definition can be found at Ind. Code § 5-14-3-4(b)(19)(j).

14 Delaware S.B. 371 (2002).

or "endanger the life or physical safety of an individual."[15]

However, using the threat of terrorism to define what infrastructure information is exempt is not without risk as illustrated in a court case from Washington, *Northwest Gas Ass'n v. Washington Utilities and Transportation Commission*. There, a narrow statutory interpretation nearly exposed Northwest Gas's pipeline location data to the public.[16]

Washington exempts security information "assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, ..." from disclosure under its Public Records Act.[17] Per Washington's Pipeline Safety Act, pipeline companies file their data with the Utilities and Transportation Commission (UTC).[18] If security data is maintained by the UTC to prevent or respond to a terrorist attack, it is exempt from disclosure.

In 2007, a Washington newspaper requested pipeline shapefile data from the UTC.[19] Northwest Gas petitioned for an injunction to exempt its shapefile data from disclosure to the newspaper.[20] The gas company supported its position with more than 20 declarations from industry personnel that pipeline system data was critical energy infrastructure, destruction of which would harm economic security and public safety.[21] The company also pointed out the pipeline served military bases.[22] Northwest Gas pointed to several exemptions in the state's Public Disclosure Act, which the legislature amended in 2005 to include a "terrorist security exemption,"[23] claiming their data fell within this exemption.

In a case of first impression, the Superior Court of Washington ruled against the injunction. Interpreting the direct text of the Act, the Superior Court did not believe the UTC specifically collected the shapefile data to respond to terrorist acts. Instead, the Superior Court found the UTC originally collected the shapefile data "to assist first responders in relationship to any incident and to coordinate with the federal government so that there would be a useable database for pipelines that carry hazardous material."[24]Accordingly, the UTC did not collect the data specifically for terrorist attacks, but for any pipeline catastrophe.[25] The Superior Court concluded, reading the exemption to include information not specific to responding to a terrorist threat was too broad.[26] Thus, Northwest Gas failed to meet the burden of proof for the exemption, and the court denied the injunction.[27] The Superior Court read the language of the exemption narrowly, stating,

15 29 Del. C. § 10002(l)(17)(a)(2).
16 *Northwest Gas Ass'n v. Washington Utilities and Transportation Comm'n*, 141 Wash. App. 98, 117, 168 P.3d 443, 454 (Oct. 2, 2007).
17 Wash. Rev. Code Ann. § 42.56.420(1).
18 *Northwest Gas Ass'n, v. Washington Utilities & Transp. Comm'n*, No. 07-2-00321-2, 2007 WL 4688058 (Wash. Super. Mar. 16, 2007).
19 Collected per Wash. Rev. Code Ann. § 81.88.080, ESRI shapefiles are digital representations of pipeline locations, pressure regulators, taps, mileposts, cathodic protection test sites, and valves. These files also contain information about diameter, pipeline operator's names, installation date, operating pressure, wall thickness, the commodity transported (such as natural gas or other substances) and other pipeline specifications. *Supra* note 18.
20 *Supra* note 16 at 449.
21 *Supra* note 16 at 443, 454.
22 *Id.*
23 Wash. Admin. Code § 42.56.420.
24 *Supra* note 18.
25 *Supra* note 18.
26 *Supra* note 18.
27 *Supra* note 18.

"The court should not be asked to turn the guiding principles of the PDA upside down by giving exemptions a broad construction."[28] The Superior Court emphasized the value of open government and freedom of information.[29] Criticizing Northwest Gas's terrorist argument, the Superior Court cautioned:

> *Over, and over again, they raise the specter of "9/11." However, we need to have the courage to use that shocking lesson, and at the same time go on to live free and democratic lives. Shall we refuse to publish ferry schedules because it would make it easier for insane terrorists to meet the boat at the dock and time an explosion?*[30]

The Court of Appeals reversed the decision. It ruled the Superior Court reading of the Public Disclosure Act was too limited, and that the result was not what the Legislature intended.[31] The appellate court held, "Although, as the trial court notes, courts should construe Public Records Act exemptions narrowly, we view its rationale here as too narrow and inconsistent with our Legislature's intent in enacting the security exemption to the Public Records Act."[32]

Unlike the trial court, the appellate court focused on the word "maintained."[33] The court reasoned, to only look at why the information was originally collected was a misreading of the exemption.[34] While the information was originally collected to aid first responders with threats to public safety, the UTC maintained the shapefile data to respond to all natural and manmade disasters, including terrorist attacks.[35]

This example illustrates that definitions matter and does legislative intent. As legislatures become more knowledgeable about cybersecurity, the definitions used to protect confidential information are growing in sophistication too.

Cybersecurity Specific Exemptions for Public Records and Meetings Laws

Recently more states are adding cybersecurity specific definitions and elements to their public records law and public meetings law exemptions. The purpose of the amendments is to address and reduce the threat of a cyberattack that uses information from publicly available documents. The following examples illustrate how states have updated public records laws to address new threats, new technologies, new actors, and new types of information. Updating the definitions gives confidence to regulators and utilities. As regulatory commissions expand their information seeking processes, they must be able to extend the protections for confidential information at the same time.

28 *Supra* note 18.
29 *Supra* note 18.
30 *Supra* note 18.
31 *Supra* note 16 at 443, 454.
32 *Supra* note 16 at 443, 454.
33 *Supra* note 16 at 119-20.
34 *Supra* note 16 at 119-20.
35 *Supra* note 16 at 119-20.

DELAWARE

In 2016, Delaware amended its public records law to add cybersecurity protections.[36] As noted above, the existing exemption was terrorism focused, and limited infrastructure protections to "telecommunications network facilities and switching equipment."[37] The new protections recognize the increased reliance of grid operators, and nefarious actors, on electric hardware and software systems. The amendment added the following to the exemptions:

> *Information technology (IT) infrastructure details, source code, logical and physical design of IT systems and interfaces, detailed hardware and software inventories, network architecture and schematics, vulnerability reports, and any other information that, if disclosed, could jeopardize the security or integrity of an information and technology system owned, operated or maintained by the State or any public body subject to the requirements of [the] Chapter.*[38]

The legislature modeled the new exemptions after the state's existing exemptions for blueprint and alarm system data, meant to prevent physical break-ins.[39] The amendment gives the Department of Technology and Information (and other public bodies subject to FOIA) the discretion to refuse to disclose the information.[40]

MICHIGAN

In 2018, Michigan amended its FOIA statute, Public Act 442 of 1976, after the Michigan State Police relayed that private victims of cybersecurity attacks were hesitant to share cybersecurity information with the police, lest it leave the entity move vulnerable if the information became public.[41] The amendment worked in three ways. First, the amendment expanded the protection against harm from just persons and property to include protections for the "confidentiality, integrity, or availability of information systems," including "cybersecurity plans, assessments, or vulnerabilities."[42] Second, the amendment specifically protected personally identifying information which could leave someone vulnerable to a "cybersecurity incident." [43] And third, the amendment clearly defined those terms while still leaving them flexible to change as cyberattack threats change.

36 Delaware S.B. 258 (2016).
37 *Id.*
38 *Id.*
39 *Id.*
40 *Id.*
41 2018 Mich. Pub. Acts 1.
42 Mich. Comp. Laws § 15.232(y) (2018).
43 Mich. Comp. Laws § 15.232(z) (2018).

Under the newly amended law, a cybersecurity plan includes, but is not limited to:

> *information about a person's information systems, network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware, or response to cybersecurity incidents.*[44]

A cybersecurity assessment is defined as:

> *"an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans."*[45]

A cybersecurity vulnerability is defined as:

> *"a deficiency within computer hardware or software, or within a computer network or information system, that could be exploited by unauthorized parties for use against an individual computer user or a computer network or information system."*[46]

A cybersecurity incident would include, but not be limited to:

> *"a computer network intrusion or attempted intrusion; A breach of primary computer network controls; Unauthorized access to programs, data, or information contained in a computer system; Or actions by a third party that materially affect component performance or, because of impact to component systems, prevent normal computer system activities."*[47]

Definitions offer clarity into the duties and obligations of parties. Flexible definitions allow the parties to adapt to changing circumstances.

IOWA

In 2017 the Iowa legislature passed two bills amending its public records law. First, the Legislature added a new exemption for cyber security information and critical infrastructure, the amendment exempted:

> *Information and records related to cyber security information or critical infrastructure, the disclosure of which may expose or create vulnerability to critical infrastructure systems, held by the utilities board of the department of commerce or the department of homeland security and emergency management for purposes relating to the safeguarding of telecommunications, electric, water, sanitary sewage, storm water drainage, energy, hazardous liquid, natural gas, or other critical infrastructure systems.*[48]

44 Mich. Comp. Laws § 15.232(c) (2018).
45 Mich. Comp. Laws § 15.232(a) (2018).
46 Mich. Comp. Laws § 15.232(d) (2018).
47 Mich. Comp. Laws § 15.232(b) (2018).
48 Iowa H.F. 445 adding Iowa Code § 22.7(70) (2017).

In the second amendment, the Legislature added a broad definition of "cybersecurity information" to that subjection. Cybersecurity information includes but is not limited to:

> *information relating to cyber security defenses, threats, attacks, or general attempts to attack cyber system operations."*[49]

The broadness of the exemption gives government agencies room to protect a variety of documents and communications relating to cybersecurity and critical infrastructure. The focus on creating vulnerabilities does not narrowly emphasize a specific type of threat or a small group of threat actors. This is the type of definition can adapt to changing circumstances as the grid evolves.

KANSAS

In 2013, Kansas amended its public records law to allow information on cybersecurity threats, attacks, or general attempts to attack utility operations to be withheld from public disclosure.[50] The amendment focuses on the possible recipients of the information from the regulatory commission to state agencies to federal organizations. The amended law covers information provided to the following entities:

> *Records of a utility concerning information about cyber security threats, attacks or general attempts to attack utility operations provided to law enforcement agencies, the state corporation commission, the federal energy regulatory commission, the department of energy, the southwest power pool, the North American electric reliability corporation, the federal communications commission or any other federal, state or regional organization that has a responsibility for the safeguarding of telecommunications, electric, potable water, waste water disposal or treatment, motor fuel or natural gas energy supply systems.*[51]

Notably, unlike the other highlighted states, the amendment focuses on the possible custodians of the information, from the regulatory commission to regional organizations to federal agencies. Additionally, the language addresses the act of a threat or the attempt to attack, rather than exempting information or records about the utility's cybersecurity protocols or other preparations. Furthermore, there is no separate definition of what constitutes a cybersecurity threat or attack.

VIRGINIA

The 2017 amendments to Virginia's public records law created a specific exemption for cybersecurity information collected by public agencies. When paired with directions on the types of communications that would be exemptible, the law offers a comprehensive protection for cybersecurity materials. The law covers:

49 Iowa Code §22.7(71) (2017).
50 Kansas S.B. 246 (2013).
51 Kan. Stat. Ann. § 45-221(54) (2013).

> "*(i) engineering, architectural, or construction drawings; (ii) operational, procedural, tactical planning, or training manuals; (ii) staff meeting minutes; or (iv) other records that reveal any of the following, the disclosure of which would jeopardize the safety or security of any person; governmental facility, building, or structure or persons using such facility, building, or structure; or public or private commercial office, multifamily residential, or retail building or its occupants*"[52]

The cybersecurity specific protections, aside from those built into the critical infrastructure protections, cover vulnerability assessments, which would allow utilities to exempt data discussing their internal monitoring and assessment programs. The law states that the following materials may be exempted:

> "*Vulnerability assessments, information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities, or security plans and measures of an entity, facility, building structure, information technology system, or software program*"[53]

The combination of content of form clarifies what types of documents warrant protection.

NORTH DAKOTA

When North Dakota amended its public records law in 2019 to cover disaster response, it added comprehensive cyber information protections.[54] Under North Dakota law, security system plans kept by a public entity and "records regarding disaster mitigation, preparation, response, vulnerability, or recovery, or for cybersecurity planning, mitigation, or threat" are now exempt from the public records disclosure requirement.[55]

Importantly, the legislature redefined key terms to acknowledge the changing nature of the grid. The amended law defined critical infrastructure as "physical and virtual" systems related to "utility services, fuel supply, energy, hazardous liquid, natural gas or coal ...."[56] As more grid operations are conducted virtually, it is incredibly valuable to have protections that extend into this sphere.

The legislature also redefined "security system plan" by adding the following language to the statute:

> (2) *Information relating to cybersecurity defenses, or threats, attacks, attempted attacks, and vulnerabilities of cyber system operations relating directly to the physical or electronic security of a public facility, or any critical infrastructure, whether owned by or leased to the state or any of its political subdivisions, or any privately owned or leased critical infrastructure if the information is in the possession of a public entity;*

52 Va. Code Ann. § 2.2-3705.2(14) (2017).
53 Va. Code Ann. § 2.2-3705.2(14)(b) (2017).
54 North Dakota S.B. No. 2209 (2019).
55 N.D. Cent. Code § 44-04-24(1) (2019).
56 N.D. Cent. Code § 44-04-24(2)(a) (2019).

(3) *Threat assessments; vulnerability*

(4) *Vulnerability and capability assessments conducted by a public entity, or any private entity; threat*

(5) *Threat response plans; and emergency*

(6) *Emergency evacuation plans.*[57]

The new definition covers mitigation, response, and recovery plans which mirrors the multiple phases of resiliency – robustness, resourcefulness, recovery, and adaptability.[58] Building a resilient system requires recognizing all the elements of resiliency and ensuring that efforts to enhance them are protected from disclosure.

NEW YORK

During the 2019-2020 legislative session, a bill was proposed, but not passed, in the New York Senate that would have enhanced operational technology cybersecurity protections by amending the definition and use of critical infrastructure information.[59] The bill defines industrial control systems as "a combination of control components that support operational functions in gas, distribution, transmission, and advanced metering infrastructure control centers, and act together to achieve an industrial objective, including controls that are fully automated or that include a human-machine interface."[60] Additionally, the bill would bring utility infrastructure protections in line with those already in place for mass transportation systems, railways, bridges and tunnels, telecommunication systems, and nuclear facilities.[61]

The inclusion of advanced metering infrastructure, automated controls, and human-machine interface is an acknowledgement of the blurring between information technology and operational technology and the growing role of technology in both. Furthermore, this new definition aligns with New York Department of Homeland Security and Emergency Services' (DHSES) understanding of critical infrastructure as anything which the "incapacitation or destruction [of] would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[62]

The legislation also envisions open communications between DHSES, the New York State Office of Information Technology Services (ITS), utilities, the public service commission (PSC) and the legislative and executive branch about the outlook of New York utilities' cyber protections. If passed, the Commissioner of DHSES and the ITS would have virtually unlimited access to review a utility's and the PSC's cyber protections. It would give these two offices access to cybersecurity reports and audits "conducted at the request of the

57 N.D. Cent. Code § 44-04-24(2)(b)(2-6) (2019).
58 *Supra* note 1 at 60.
59 New York, S. 6195 2019-2020 Regular Sessions.
60 New York, S. 6195, §3 2019-2020 Regular Sessions.
61 New York, S. 6195, §4 2019-2020 Regular Sessions.
62 GovTech, New York Legislation Seeks to Block Energy Grid Cyberattacks, May 10, 2019. https://www.govtech.com/policy/New-York-Legislation-Seeks-to-Block-Energy-Grid-Cyberattacks.html.

public service commission or any other agency or authority of the state or any political subdivision thereof or, to the extent practicable, of any federal entity."[63]

Public Meetings

Public meetings laws, known as open meetings laws or sunshine laws, are laws that provide access to meetings of government boards, councils, commissions, and other entities. Public meetings laws can require government bodies to meet and deliberate in public, provide access to notes and minutes taken at those meetings, and provide access to all decisions and reports. The exact form of the public meetings law will differ by state.[64] Depending upon the state, the discursive and deliberative functions of the public utility commissions may be subject to public meetings laws. Efforts to build information sharing between the commission and its regulated utilities may elicit utility concern that the public meetings requirement will interfere with the protection of confidential information.[65]

Alignment of public records laws with public meeting laws is a simple way to facilitate the exchange of documents and to create platforms for discussing confidential information. When utility commissions engage in discussions with their utilities on their cybersecurity posture, a single set of rules builds confidence in the level of protection.

FLORIDA

Florida, known for having one of the most expansive public meetings laws,[66] recently exempted from disclosure public utility commission meetings that discuss utility information technology and industrial control systems.[67] Under the revised statute, the following types of information are exemptible, "information related to the security of the technology, processes, or practices" for the purpose of protecting a utility's information technology; protecting information about industrial control systems which if made publicly available could jeopardize the technology or reliability of the system; and safeguarding customer meter-data.[68]

The newly amended statute aligned the public meetings law with the public records law.[69] The Legislature found, as a matter of public necessity, if the utility's information would be exempt under Florida's public records law, it is should also be exempt from disclosure at public meetings.[70] The changes to the public records law in 2016 and the public meetings law in 2019 stemmed from the legislature recognizing that the grid is more interconnected than ever before, and the harm of disclosure outweighed any public benefit from that disclosure.[71]

63 *Supra* note 59.
64 Middle Tennessee State University, The First Amendment Encyclopedia, Open Meeting Laws and Freedom of Speech, https://www.mtsu.edu/first-amendment/article/1214/open-meeting-laws-and-freedom-of-speech.
65 *Supra* note 1 at 22.
66 Under Florida law, all meetings of any board of commission of any state agency or authority or of any county, municipality, or political subdivision, unless exempted by the Constitution, are subject to the public meeting laws, Fla. Stat. § 286.011.
67 Fla. Stat. § 286.0113(a).
68 *Id.* citing to FLA. STAT. § 119.0713(5)(a)(1-3) (public records requests).
69 The legislature amended the public records law in 2016 see Florida C.S.C.S.H.B. 1025 (2016).
70 Florida H.B. 00327, §2(1).
71 Florida H.B. 00327, §2(2)(b)(2)-(3).

Step 2: Limiting Commission Access to Confidential Information

One of the ways utility commissions manage confidential information is by limiting their access to the information, by constraining where they access the information, or by restricting who within the Commission can access the information. Rather than seeking protection for information received, commissions have developed strategies for reducing the amount of information held by them or within their control. For example, commissions have avoided receiving granular-level data that might reveal system vulnerabilities. Commissions have limited attendance and note taking at meetings where cybersecurity programs are discussed. Commissions have also moved audit and investigatory proceedings to utility property and avoided bringing utility documents under commission control, see Section 3. Lastly, Commissions have used non-disclosure agreements to bind parties receiving critical infrastructure information.

Limiting Collection of Confidential Information

Utility commissions collect information to help them assess and evaluate utility performance. For many commissions and utilities, the response to the concern about the vulnerability created by exchange and storage of the information has been to constrain information collection. Some commissions limit the types of information that a utility must provide. The commissions still want evidence that a utility is maintaining an active cybersecurity risk management program, but they do not want to collect information that if released would increase the vulnerability of the utility.

This type of system can make effective use of limited commission resources. However, as the commission gains institutional familiarity and capacity with cybersecurity, it should re-evaluate the effectiveness of maintaining the information imbalance between itself and the utility.

DELAWARE

The Delaware Public Service Commission tailored its reporting requirements to minimize the collection of sensitive information. The Commission requires utilities to submit an annual cybersecurity questionnaire, which provides high-level information, rather than undergo stricter reporting requirements. The annual questionnaire meets the goals of the Commission of avoiding duplicative regulation and balancing open communication between the Commission and utilities, while protecting confidential information.[72] The questions are broad enough to protect sensitive information. Most questions are yes or no questions, asking generally whether certain plans are in place, rather than requiring the utilities to go into the details of the plans.[73]

72 Delaware PSC Docket 16-0659, Staff Memorandum/Draft Order September 28, 2016, In the Matter of the Commissions' Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Investor Owned Electric, Gas and Water, Oct. 12, 2016 at 2.

73 *Id.* at 2-3.

The form and structure of the reporting requirement was the product of a deliberative process. The Commission opened a cybersecurity docket in May 2016.[74] The Commission used the docket to review its legal obligations to public safety, other jurisdiction's cybersecurity regulations, and solicited input from the regulated utilities, PJM, the Delaware Division of Public Advocate, and Staff.[75, 76] At the conclusion of this research, the Commission determined reporting regulations or guidelines were unnecessary as the utilities were already hiring new cybersecurity employees, working with outside firms to audit their systems, and following the NIST framework.[77] Additionally, Staff reported the utilities were working with FERC, the FBI, and DHS.[78]

KENTUCKY

In Kentucky, the Public Service Commission's decision to limit collection of information developed over the course of two grid modernization orders.[79] In both cases, the Commission identified cybersecurity as an essential part of a functioning modern grid while the utilities, in unanimity, argued that the Commission should not adopt new regulations or binding requirements. The utilities argued existing national and regional mandatory and voluntary cybersecurity standards were enough to ensure strict protocols, warning state level reporting could risk confidential and sensitive plans.[80] Further, the utilities maintained that additional regulations could "weaken rather than strengthen utilities' ability to thwart cyber-attacks by slowing their ability to adapt to the ever-changing threat."[81] Given this concern, the Commission and the Attorney General agreed the information should be kept internally by the utility.

The decision not to collect information did not alleviate the utilities from providing information to the Commission. When the Commission exercised its discretion to not require utilities to file information about their internal procedures, it imposed a requirement to certify the development of those procedures and present to the Commission.[82] Additionally, if a utility still believes the information requested from the Commission could result in injury, the utility can petition to the Commission to exempt that information from public disclosure.[83] For example, the Commission granted Duke

74 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.

75 *Id.* at 2.

76 Delaware PSC Docket 16-0659, Public Workshop Minutes Aug 18th, In the Matter of the Commissions' Review of the Necessity for Cybersecurity Guidelines or Regulations for Delaware Investor Owned Electric, Gas and Water, September 1, 2016.

77 *Supra* note 72 at 2-3.

78 *Supra* note 72 at 3.

79 Kentucky Public Service Commission, Case No. 2012-00428, In the Matter of: Consideration of the Implementation of Smart Grid and Smart Meter Technologies; Kentucky Public Service Commission, Case No. 2008-00408, In the Matter of: Consideration of the New Federal Standards of the Energy Independence and Security Act of 2007.

80 Kentucky Public Service Commission, Case No. 2012-00428, Order, In the Matter of: Consideration of the Implementation of Smart Grid and Smart Meter Technologies at 29.

81 Kentucky Public Service Commission, Case No. 2012-00428, Joint Utilities Brief, In the Matter of: Consideration of the Implementation of Smart Grid and Smart Meter Technologies, February 27, 2015 at 8.

82 *Supra* note 80 at 29.

83 Ky. Rev. Stat. Ann. § 61.878(1)(c)(1), see Kentucky Public Service Commission, Case No. 2012-00428, Order, In the Matter of Consideration of the Implementation of Smart Grid and Smart Meter Technologies, January 17, 2019.

Energy Kentucky an exemption to the public records law for information which could expose vulnerabilities and threaten public safety. Duke argued the information requested were "internally-derived policies that would give competitors, hackers, or others sensitive information and cause a threat to Duke Energy Kentucky's cyber security system it has in place."[84]

Limiting Retention of Confidential Information

Limiting control of confidential information is another tool used by utility commissions to reduce cybersecurity risks without impairing the commission's insight into utility cybersecurity posture. Public records requests and public meetings requests seek information that is held by or within the control of an agency. If the information remains in the possession of the utility, it is not accessible via a public records request. Commissions have taken advantage of the legal interpretation of control by tailoring their interactions with utilities to gain access to information without gaining control of the information.

CONNECTICUT

In Connecticut, sensitive cybersecurity information is protected by the Public Utilities Regulatory Authority's (PURA) Cybersecurity Oversight Program and by state and federal statutes. The Oversight Program protects confidential information by restricting the number of participants, using off-site meetings and non-disclosure agreements (NDAs), and limiting the collection of records.

The Program requires annual meetings between the utilities and regulators for the purpose of assisting PURA in understanding the utilities' strengths and weaknesses. The goal of the meetings is to develop that understanding rather than requiring a utility to demonstrate it is meeting prescribed standards.[85] To ensure the meetings are candid, the Commission allows the utility to guide where the meeting will go, and who will be in attendance. Unless the utility determines otherwise, the meetings are limited to the utility, PURA, and the Division of Emergency Management and Homeland Security (DEMHS) representatives.[86] Additionally, the meetings are held at the utility's office rather than an agency office and attendees are bound by non-disclosure agreements.[87] Finally, since neither PURA nor DEMHS take custody of the information shared, the utility retains all information.[88]

State sunshine laws complement that the procedural and custody protections crafted by PURA.[89] State law allows for the Commissioner of the Department of Administrative Services and the PURA agency head to exempt records or internal processes when they

84 Kentucky Public Service Commission, Case No. 2012-00428, Duke Energy Kentucky's Response to Attorney General's Data Requests and Response to Commission's Data Requests, In the Matter of: Consideration of the Implementation of Smart Grid and Smart Meter Technologies, March 20, 2013 at 2.

85 State of Connecticut, Public Utilities Regulatory Authority, Docket No. 14-05-12, Connecticut Public Utilities Cybersecurity Action Plan, April 6, 2016 at 21-25.

86 *Id.* at 24.

87 *Id.* at 24-25.

88 *Id.* at 24-25.

89 *Id.* at 25.

have a reasonable belief disclosure could pose a safety risk to people or government-owned property, or "which would compromise the security or integrity of an information technology system."[90]

NEW YORK

Similarly, in New York, the information gathered by auditors from the Office of Utility Security remains in the physical offices of the utilities during the quarterly physical and cybersecurity audits.[91]

Step 3: Balancing the Public Interest

Information protections must be balanced with access to information. The public's right to participate in critical infrastructure planning processes and comment on utility investment proposals is a central part of the bargain between regulated utilities and their ratepayers. The sensitive nature of critical infrastructure information and, particularly, cybersecurity information can push for higher levels of protection and less disclosure to the public. Maintaining the balance between access and protection is tricky, but states continue to develop and apply techniques for navigating this dilemma.

The following examples present four state records law specifically addressing cybersecurity and how two utility commissions have approached requests to classifying confidential information. The states profiled avoided blanket exemptions by providing a process for classifying information that is paired with a process for requesting information. Amongst the tools used by the states are specificity of definition and burden of proof. Clear definitions create clarity for what information is and is not covered by the statute or regulation. Placing the burden of requesting and defending the request on the party seeking the protection avoids creating an administrative burden that can tilt the relationship between accessibility and security.

The final two examples demonstrate how a commission can navigate the tension between accessibility and risk avoidance. Quick action can ease utility concerns, but the decision to exempt information from disclosure must be justifiable.

ALABAMA

In Alabama, the state agency plays a gatekeeper role in granting access to critical infrastructure information and critical energy infrastructure information. A blanket exemption is not provided, but the owner of the information is given the opportunity to comment on the request and justify its exemption. Under Alabama law, when the public officer receives a request for records that "may appear to relate to critical infrastructure or critical energy infrastructure information," the officer must notify the owner of the information and provide an opportunity to comment on the request and on the public safety and welfare threats that could reasonably arise from publicly disclosing the records.[92]

90 Conn. Gen. Stat. § 1-210(b)(19)-(20).
91 *Supra* note 1 at 24.
92 *Supra* note 11.

VIRGINIA

Similarly, Virginia provides a detailed statutory process for requesting information be withheld from disclosure. Under Virginia law, there is an expectation that records submitted to a public body, including records for the purpose of antiterrorism response planning or cybersecurity planning or protection, will be disclosed upon request.[93] However, the records may be withheld from disclosure if:

> *such person or entity in writing (a) invokes the protections of this subdivision, (b) identifies with specificity the records or portions thereof for which protection is sought, and (c) states with reasonable particularity why the protection of such records from public disclosure is necessary to meet the objective of antiterrorism, cybersecurity planning or protection, or critical infrastructure information security and resilience.*[94]

Requiring entities to request the protection is a common element of public records laws. Protections are afforded to those who request them, otherwise the presumption is that the materials are for public disclosure. As will be shown in the New Hampshire example, who can exert the request for protected status varies and, in some situations, the state agency is able to classify documents that it receives from a utility without requiring the utility to submit a formal request.

NEW HAMPSHIRE

Under New Hampshire law, all records submitted to the New Hampshire PUC for adjudicative and non-adjudicative proceedings are deemed to be in the public record.[95] New Hampshire allows utilities to request confidential treatment of the routine cybersecurity records they submit.[96] The utility must still submit a public version and a confidential version of the utility's records[97] and if there is a request for public release of the confidential version, the Commission makes that determination, weighing the interests of the utility and the potential for social harm against the request.[98]

The Commission also has the power to eliminate confidentiality concerns at the beginning of a proceeding. The Commission can offer a pre-classification of information to be received, thus providing notification of the status of the information to the utility and to the public. For example, in a recent Liberty Utilities petition to approve a battery storage pilot program, the Commission requested a comprehensive evaluation of the cybersecurity risks, vendor's practices, detection methods, and mitigation strategies.[99] The Commission gave advance notice to the utility that the submission of the plan for the pilot program

93 Va. Code Ann. § 2.2-3705.2(14)(d).
94 *Id.*
95 N.H. Code Admin. R. Ann. PUC 201.04.
96 N.H. Code Admin. R. Ann. PUC 201.06(a)(16).
97 N.H. Code Admin. R. Ann. PUC 201.06(b).
98 N.H. Code Admin. R. Ann. PUC 201.06(c-d).
99 New Hampshire Public Utilities Commission, DE17-189, Order Approving Settlement Agreement and Implementation of Pilot Program and Granting Motions for Confidential Treatment, January 17, 2019 at 40.

would receive confidential treatment.[100] The advance notification can streamline the submission process and reduce administrative costs.

CALIFORNIA

Public utility commissions can also be arbiters of whether an exemption from disclosure request is overbroad. Under California law, the Public Utility Commission must use a public interest balancing test to determine whether the public interest is best served by not disclosing the information. This test was at the center of a recent Commission decision on exempting critical infrastructure information from disclosure.[101] The decision highlights how the burden for exemption should be placed on the requesting party and that exemptions can be narrowly tailored to serve the public interest.

In 2013, Assembly Bill 327 amended the Public Utilities Code to require that electric utilities file Distribution Resource Plans with the Commission.[102] The legislature's goal was to provide interested parties the ability to "identify optimal locations for the deployment of distributed resources."[103] To meet this objective, the Commission opened Rulemaking 14-08-13.[104] The Commission required Pacific Gas & Electric, Southern California Edison, and San Diego Gas and Electric (the Utilities) to include an overlay of additional sensitive information to the distributed resources plan and make it available in an online, downloadable map.[105]

The Utilities petitioned that this data should be confidential on physical or cybersecurity grounds, relying on Government Code §6255(a), the "public interest balancing test." The test requires the Commission to find "the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record."[106] That is, the utility must demonstrate a "clear overbalance" to keep the data confidential.[107] The Commission held the Utilities did not meet this burden.[108]

The Commission's decision highlighted the burden of specificity borne by utilities. When an entity uses Government Code §6255(a) to keep information confidential, it must "demonstrate with granular specificity on the facts of the particular information why the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record."[109] The Utilities' comments that "the physical location of all IOU electric distribution facilities, including substations, feeders and circuits, would be

100 *Id.* at 40.
101 California Public Utilities Commission, Rulemaking 14-08-013, Order, Instituting Rulemaking Regarding Policies, Procedures and Rules for Development of Distribution Resources Plans Pursuant to Public Utilities Code Section 769, December 17, 2018.
102 California Public Utilities Commission, Rulemaking 14-08-013, Distribution Resources Plan, Proceeding Overview, August 13, 2014.
103 California A.B. 327 (2013) at 32.
104 California Public Utilities Commission, Rulemaking 14-08-013, Order, Instituting Rulemaking Regarding Policies, Procedures and Rules for Development of Distribution Resources Plans Pursuant to Public Utilities Code Section 769, August 14, 2014.
105 California Public Utilities Commission, Rulemaking 14-08-013, Administrative Law Judge's Ruling Resolving Confidentiality Claims Raised by Pacific Gas & Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company as to Distribution System Planning Data Ordered by Decision D. 17-09-026 and D. 18-12-2004, December 17, 2018 at 2-4.
106 Cal. Government Code § 6255(a).
107 *Michaelis, Montanari & Johnson v. Superior Court*, 38 Cal. 4th 1065, 1071 (2006).
108 *Supra* note 102.
109 California General Order 66-D §3.2(b), September 28, 2017.

subject to the NDA, as well as all related safety-and-security-sensitive data,"[110] did not meet the burden because it failed to explain why this information should not be available to the public.[111] Southern California Edison cited to FERC's definition of CEII but did not explain how each of its components fit that definition.[112] Finally, the explanations did not set apart what information the Utilities wanted protected from what was already made publicly available.[113] Thus, the Commission held that the Utilities failed to meet this specificity requirement.[114]

The Commission recognized that California was concerned with protecting CEII from cybersecurity threats but recognizing that concern is not the equivalent of demonstrating with factual specificity why the locations of distribution substations, circuits and feeders, as identified on the maps should be classified.[115] Citing a 1988 CPUC case, the Commission reminded the parties that "[t]he burden of proof that must be established in order to restrict access to information is a rigorous one since the strong public interest in an open Commission process will outweigh the unsubstantiated claim of confidentiality."[116]

Conclusion

Sharing and protecting critical infrastructure confidential information is at the heart of every effort to improve distribution utility cybersecurity preparedness. Addressing security concerns in information sharing processes builds trust between utilities and their regulators. That trust becomes that foundation for actions that mitigate risk and boost responsiveness. Utility commissions need better information to understand utility investment proposals, to evaluate system weaknesses, and to develop proactive dockets. However, the act of creating and sharing the information increases the risk to the security of the grid.

The examples presented in this section demonstrate that there are pathways for improving the flow of information without adding to the vulnerability of the grid. The first step starts with definitions that reflect the nature of the changing grid and the emergence of cyber threats. States are actively crafting processes and protocols that facilitate information flows between regulators and utilities without adding risk to the system. Moreover, protections can be built while balancing the public's right of access to information. Sharing and protecting information creates the trust that fuels actions that reduce risk and enhance system resiliency.

110 California Public Utilities Commission, Rulemaking 14-08-013, Joint Periodic Status Report of Pacific Gas and Electric Company (U 39 E), San Diego Gas & Electric Company (U 902 E), Southern California Edison Company (U 338 E) Pursuant to November 9, 2018, Administrative Law Judge's Ruling, November 16, 2018 at 5.

111 *Supra* note 105.

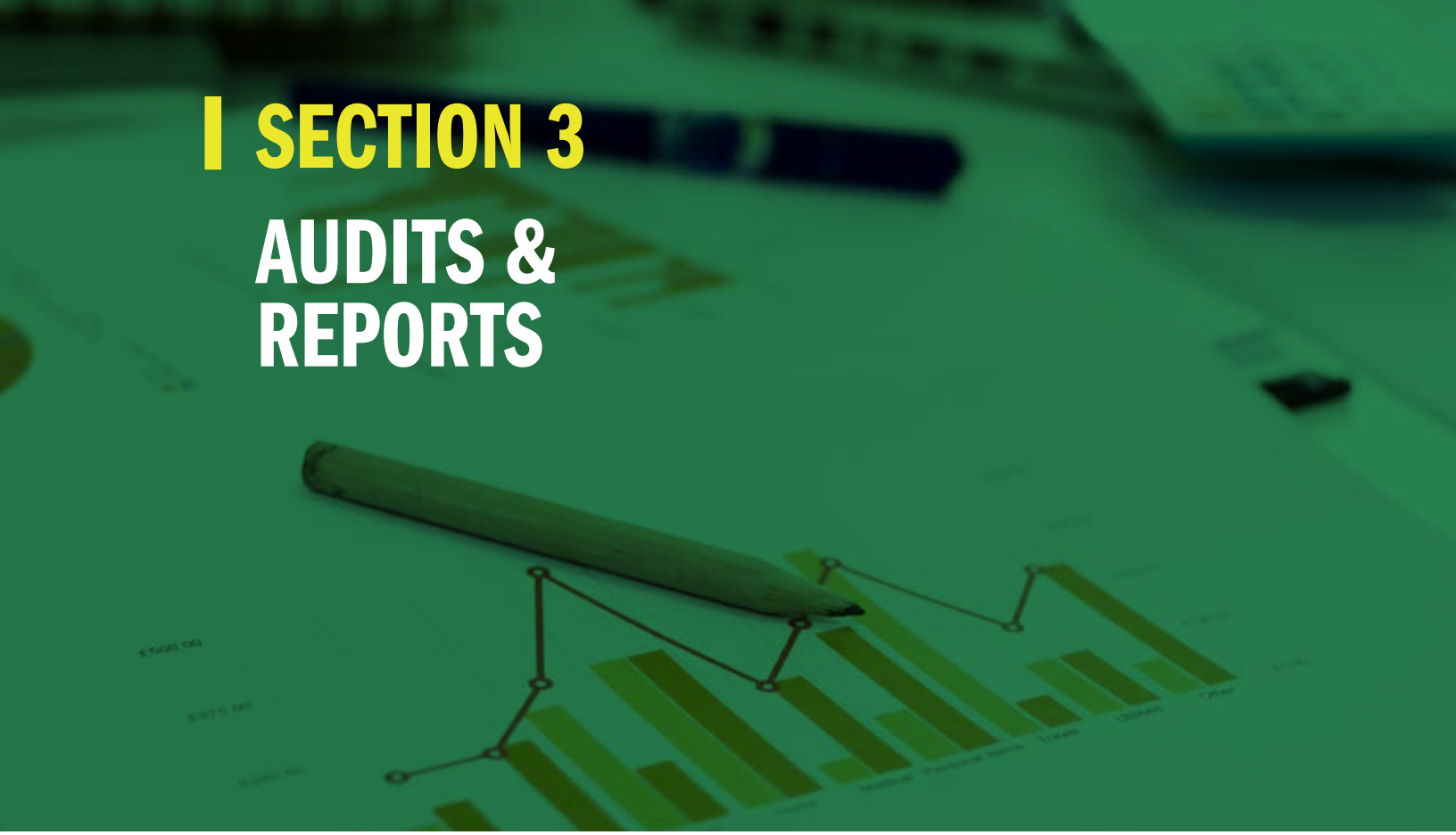
112 California Public Utilities Commission, Rulemaking 14-08-013, Motion of Southern California Edison Company (U 338-E) for Confidential Treatment and Redaction of Distribution System Planning Data Ordered by Decisions D.17-09-026 and D. 18-02-004, June 15, 2018 at 7.

113 *Supra* note 102 at 12.

114 *Supra* note 102.

115 *Supra* note 102 at 10.

116 *Supra* note 102 at 11 citing Re Sierra Pacific Power Company (1988) 28 CPUC 2d 3.



SECTION 3
AUDITS & REPORTS

THE INFORMATION ASYMMETRY that exists between utilities and their regulators on cybersecurity threats, vulnerabilities, practices, policies, and processes is a serious obstacle to elevating grid security and resiliency.[117] The asymmetry exists because there is an imbalance in knowledge. Utilities, who are at the forefront of daily efforts to prevent cyber intrusions and attacks, have a scope and depth of knowledge that greatly exceeds that of their regulators. By reducing this imbalance, primarily through the exchange of information from the utility to the regulators, regulators can gain deeper understanding of utility practices and policies. That understanding is essential to evaluating and assessing investment proposals and policy decisions.

Utility commission reporting and auditing processes are existing, commonly used practices that can help bridge the information asymmetry.[118] The infrastructure already exists to collect, process, and assess reports. The authority to conduct audits is well-tested and the processes are well-honed. Reports and audits allow utility commissions to assess utility investments, evaluate progress in implementing plans, and provide feedback to guide future decisions.

Orienting the structure of the reporting requirement or the audit procedure to

117 In the Phase 1 report, multiple interviewees identified information asymmetry as a major barrier to improving cybersecurity protections. *Supra* note 1 at 21.

118 Information exchange can be done through formal structures or informal practices. This Section focuses on formal structures while encouraging all methods that improve communication and information flow. For more information on informal practices, see Section 2 - Critical Infrastructure Confidential Information.

accommodate cybersecurity is a critical task for utility commissions. Utility commissions employing reporting requirement and audit processes should focus them to seek out best practices. Reports can have a backwards-looking lean, discussing what actions have been taken and what progress has been made. That information is valuable, but there is also value in reports that feed into future decision making. Reporting requirements should feed into a planning process to determine what next steps are required to secure the grid. Similarly, audits can evaluate past performance and identify needed changes. Audits can also scrutinize management practices and processes, providing a holistic view of a utility's cybersecurity posture. The strategic use of metrics can assist in identifying key system attributes and in measuring system performance.[119]

The attack surface of the distribution system is increasing due to the digitization of operational control and the connection of millions of new devices. System vulnerability evolves as these changes are manifested and, consequently, risk management best practices need to follow along. A static reporting requirement will not generate the same amount or quality of information as a reporting requirement that obliges utilities to update actions taken and provide explanations on how they are using the information to improve their management practices.

The reports and audits should be designed to minimize the exposure of critical infrastructure confidential information.[120] Reporting and audit processes should be crafted to maximize the flow of information between secured parties while minimizing the risk of exposure. Information gathered from the reports and audits on best practices can also be shared between utilities, thus elevating the cybersecurity posture of the entire industry. Structured information sharing opportunities can also help negate some of the information asymmetry that exists between larger and smaller distribution utilities.

This section identifies three formal processes employed by utility commissions that can reduce the information asymmetry that limits actions on cybersecurity. Each of the processes draw upon existing commission authority to regulate their jurisdictional utilities. The processes, when deployed, create regular information sharing practices on cybersecurity preparedness and evaluate cybersecurity performance. The practices are:

1. Cybersecurity Reports
2. Smart Grid Reports
3. Management and Operations Audits

Cybersecurity Reports

Utility commissions are seeking more information on the cybersecurity posture of the utilities that they regulate. The commissions want to know how their regulated utilities are addressing emerging threats, what actions the utilities are taking to identify and mitigate system vulnerabilities, how utilities are training their staff, what investments they are making to reduce vulnerabilities, and how they are measuring system performance. This subsection highlights recent actions taken in Michigan and Maryland to introduce mandatory cybersecurity specific reporting requirements and it presents recent legislative changes in Texas that create a cybersecurity monitor to review voluntary self-assessments.

119 For more information on metrics, see Section 5 of the report.

120 See Section 2 of the report for more detail on critical infrastructure confidential information.

The approaches of Maryland and Michigan share many similarities, while differing slightly on substance and the reporting process. Both Maryland and Michigan seek general overviews of their utilities' approach to cybersecurity planning and awareness as well as information on training programs and risk management processes. Maryland requests greater detail on the management of third-party risks, an important consideration as more services move to the cloud amidst a growing role for third-party vendors. Additionally, Maryland mandatory reporting requirement categories are derived from NARUC's 2017 Cybersecurity Primer, "A Primer for State Utility Regulators,"[121] and the CSRWG included questions from the Primer in its final report as a guide for utilities submitting their reports and regulators evaluating the reports.[122]

Both states seek information on how cybersecurity preparedness is integrated into a utility's response and recovery planning. Resiliency means more than investing in mitigation and protection efforts. A resilient system must be able to respond to an incident to minimize damage and to quickly restore service to affected customers. Requiring reporting on all elements of cyber preparedness broadens the perspective of the utility and the regulators and creates an opening for discussion on interactions with other agencies.

Lastly, each state requires that the reports are accompanied by a briefing. Michigan offers utilities the ability to present orally in writing and to present in groups. This design has two-fold benefits. First, it creates opportunities for inter-utility information exchange. Second, it minimizes document retention which is a key element in reducing access to critical infrastructure confidential information.

MICHIGAN

In early 2019, new cybersecurity reporting rules came into place for Michigan's investor-owned utilities and member-owned cooperatives. The rule change started in 2017, when the Michigan Public Service Commission self-initiated an update of its Technical Standards for Electrical Service,[123] after the standards had gone more than a decade without an update.[124] The revised standards update several areas including technical requirements for electricity meters, meter inspections, customer relations, and tests. The Commission proposed and received approval to add a new reporting requirement, Security Reporting,[125] that required utilities to present information about their cybersecurity program and related risk planning/threat assessment and preparedness strategy.

The new reporting requirements apply to investor-owned utilities and member-owned

121 Maryland Public Service Commission, Order No. 88499, Report of the Cyber-Security Work Group, Proposal for Addressing the Cyber-Security Reporting Process for Maryland Utilities, April 6, 2018 at 8 citing Miles Keogh and Sharon Thomas, National Association of Regulatory Utility Commissioners, Cybersecurity: A Primer for State Utility Regulators Version 3, January 2017, https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

122 Miles Keogh and Sharon Thomas, National Association of Regulatory Utility Commissioners, Cybersecurity: A Primer for State Utility Regulators Version 3, January 2017, https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F at 15.

123 Under the Michigan Administrative Procedures Act of 1969, state agencies are authorized to promulgate rules that implement or apply law enforced or administered by the agency.

124 Michigan State Budget Office, Office of Regulatory Reinvention, Agency Report to the Joint Committee on Administrate Rules (JCAR), 2017-091-LR, February 12, 2018 at 1.

125 Mich. Admin. Code r.460.3205 (2019).

cooperatives, both of which fall under the jurisdictional purview of the Commission.[126] However, the reporting responsibilities vary with IOUs receiving additional reporting requirements on major investments in the past year, and the plans and rational for anticipated major investments in the coming year.[127] The mandated contents of the report and the method of delivery of the report allow for the Commission to receive a comprehensive picture of the utility's cybersecurity posture while simultaneously providing an avenue for limiting the chance of disclosing sensitive information. Lastly, utilities may petition to be exempted from the reporting requirement, but the presumption is that utilities will comply unless they can show good cause for a waiver or exception.[128]

Report Contents

A reporting utility must provide a general overview of its program, descriptions of training programs, an organizational diagram of its cybersecurity organization, a description of its communication plans, summaries of breach events, a description of risk assessment tools and methods and how they are used to improve utility performance and capabilities, and general information about emergency preparedness plans including threat and vulnerability assessments. A complete listing of filing requirements is below:

i. *An overview of the program describing the electric provider's approach to cybersecurity awareness and protection.*

ii. *A description of cybersecurity awareness training efforts for the electric provider's staff members, specialized cybersecurity training for cybersecurity personnel, and participation by the electric provider's cybersecurity staff in emergency preparedness exercises in the previous calendar year.*

iii. *An organizational diagram of the electric provider's cybersecurity organization, including positions and contact information for primary and secondary cybersecurity emergency contacts.*

iv. *A description of the electric provider's communications plan regarding unauthorized actions that result in loss of service, financial harm, or breach of sensitive business or customer data, including the electric provider's plan for notifying the commission and customers.*

v. *A redacted summary of any unauthorized actions that resulted in material loss of service, financial harm, or breach of sensitive business or customer data, including the parties that were notified of the unauthorized action and any remedial actions undertaken.*

vi. *A description of the risk assessment tools and methods used to evaluate, prioritize, and improve cybersecurity capabilities.*

vii. *General information about current emergency response plans regarding cybersecurity incidents, domestic preparedness strategies, threat assessments, and vulnerability assessments.*[129]

126 The Michigan Public Service Commission has jurisdiction to regulate all public utilities in the state except municipally owned utilities, some types of owners of renewable energy production facilities, and specifically exempted entities. Mich. Comp. Laws § 460.6(1) (2005).

127 Mich. Admin. Code r.460.3205(1)(b) (2019).

128 Mich. Admin. Code r.460.3101(5).

129 Mich. Admin. Code r.460.3205(a) (2019).

Other additional responsibilities include a duty to report intentional interruptions of production, transmission, or distribution of electricity; extortions done through cyberattacks; denial of service attacks lasting longer than 12 hours; and the access or theft of data that compromises security or confidentiality of personal information.[130] Additionally, the utility, at its discretion, may report any other "cybersecurity incident, attack, or threat which the electric provider deems notable, unusual, or significant."[131]

Flexible Reporting Options

The rule takes specific steps to protect the information collected in the reports. Under the enacted rule, utilities have the option of providing a written or an oral report to the designated Commission staff.[132] Designating which staff will receive the reports reduces the number of parties with access to the information, which is an simple method for protecting confidential information. Additionally, an oral report can avoid the creation of a record subject to public disclosure. However, the public meeting laws may be subject to Michigan's Open Meetings Act,[133] and a petition to exempt sensitive information would be required.

The reporting options acknowledge the reporting burden and the differences in utility capacity. The Public Service Commission has full regulatory authority over Michigan's investor-owned utilities and partial authority of some elements of the operations of the member-owned cooperatives.[134] The information asymmetry that exists between utility and utility regulator also exists between utilities of different sizes and different capacities. Of Michigan's investor-owned utilities, two – Consumers Energy and DTE Energy, both serve in excess of 1.8 million electric customers.[135] Utilities have the option of presenting individually or jointly.[136] This option acknowledges the benefit of having a platform for multi-party discussions. The flexibility in the reporting format opens the door to inter-utility information sharing that could collectively raise the cybersecurity posture of all Commission-regulated utilities.

130 Mich. Admin. Code r.460.3205(2)(a)-(d) (2019).
131 Mich. Admin. Code r.460.3205(2)(e) (2019).
132 Mich. Admin. Code r.460.3205(1)(a) (2019).
133 Michigan Attorney General, Open Meetings Act Handbook, https://www.michigan.gov/documents/ag/OMA_handbook_287134_7.pdf.
134 Michigan Public Service Commission, About the MPSC - Electricity, https://www.michigan.gov/mpsc/0,9535,7-395-93218_93299-499212--,00.html. The Commission has full oversight of the investor-owned utilities and regulates the safety and reliability of the cooperatives.
135 Consumers Energy serves 1.8 million customers, Consumers Energy, About CMS Energy, https://www.cmsenergy.com/about-cms-energy/consumers-energy/default.aspx and DTE Electric Company serves 2.2 million customers, DTE, About DTE, https://newlook.dteenergy.com/wps/wcm/connect/dte-web/home/about-dte/common/about-dte/about-dte.
136 *Supra* note 132.

MARYLAND

On February 4, 2019, the Maryland Public Service Commission adopted new comprehensive cybersecurity reporting and briefing requirements.[137] The new requirements replaced a pre-existing cybersecurity reporting program for Baltimore Gas & Electric and Pepco that was established in 2013 during proceedings to authorize the deployment of smart grid technology.[138]

The new reporting requirements were the conclusion of a year-and-half process. In December 2017, the Commission ordered the creation of the Cyber-Security Reporting Work Group (CSRWG). The CSRWG was compromised of representatives from Maryland utilities, the Office of the People's Counsel, and the Commission.[139] The CSRWG was tasked with producing a report with a series of recommendations on how to further advance the Public Service Commission's cybersecurity reporting program.[140] The CSRWG produced a list of recommendations, adopted by the Commission with minor changes, that expanded and clarified the cybersecurity briefing and reporting responsibilities of Commission-regulated utilities.[141]

The Commission initiated the review based on concern about risk. The risks arising from the automation of distribution grid systems had grown considerably since 2013 as had threats to the physical infrastructure.[142] Smart grid deployment in Maryland had expanded beyond the two utilities affected by the 2013 order which has changed the potential attack surface of the grid.[143] Also, new research into distribution grid cybersecurity was not being incorporated into the existing requirements and thus the existing requirements may be lagging behind best available practices.[144] In light of the changing circumstances, the Commission sought to review whether the existing requirements were adequate to protect and maintain the safety and security of the distribution grid.

Report Contents

The new reporting requirements take a broader, more progressive approach to cybersecurity by focusing on the changing nature of cybersecurity threats. The old reporting requirements focused on advanced metering infrastructure and data privacy. In promulgating the new reporting requirements, the Commission noted that cybersecurity protection must encompass information technology, operational technology, and industrial control systems plus smart grid systems.[145] The Commission also used the order to define Information Technology System (IT System), Operational Technology System (OT

137 Maryland Public Service Commission, Order No. 89015, In the Matter of Cyber-Security Reporting of Maryland Utilities, Case No. 9492, February 4, 2019.
138 Maryland Public Service Commission, Order No. 85680, In the Matter of Potomac Electric Power Company and Delmarva Power and Light Company Request for the Deployment of Advanced Meter Infrastructure, Case No. 9207, June 21, 2013.
139 *Supra* note 121 at 14.
140 *Supra* note 121.
141 *Supra* note 137.
142 Maryland Public Service Commission, Case No. 9207, Case No. 9208, Order 88499, December 11, 2017 at 2.
143 *Id.*
144 *Id.* The Commission specifically noted the cybersecurity work done by NARUC and the U.S. Department of Energy.
145 *Id.* at 3.

System), Smart Grid System, and Security Breach.[146] The definitions clarified the new responsibilities and duties of the utilities to monitor and report on their systems.

The order directed the structure of future briefings by the utilities to the Commission. The period Cyber-Security reports must include the following ten categories:

i. *Cyber-security Plan Overview;*
ii. *Cyber-security Standards Adopted;*
iii. *Reporting Cyber Incidents;*
iv. *Partnerships for Information Sharing, Planning, and Situational Awareness;*
v. *Procurement Practices to Manage Cyber-security Risks from Vendors;*
vi. *Personnel and Policies on Hiring, Training, and Separation to Manage Cyber-security Risks;*
vii. *Risk Management Process to Assess and Prioritize Cyber-security Risk;*
viii. *Implementation of Cyber-security Strategies;*
ix. *Response and Recovery to Cyber Incidents; and*
x. *Cyber-security Process.*[147]

Briefing Procedures

Many of the older procedural requirements were retained, while new elements were added to address confidential information protections and reporting burdens. Confidential information is protected in a couple of ways. First, the number of parties who can see the report without having a government security clearance is restricted.[148] Those parties are specifically designated in the order as Cyber-Security Authorized Representatives.[149] Cyber-Security Authorized Representatives will not have access to detailed information requiring a government security clearance and they are subject to Maryland law preventing individuals from disclosing information learned while inspecting a utility facility or examining the records a public service company.[150] Second, access to briefing materials is restricted. Materials circulated at a periodic briefing with the Commission are collected at the end of the briefing and retained by the utility.[151]

Under the new protocols, briefing and reporting responsibilities vary depending upon the size of the utility. The periodic briefing requirements apply to all water, gas, and electric utilities regulated by the Commission and serving more than 30,000 Maryland customers.[152] Utilities subject to the briefing requirements must periodically file briefs with the Commission in accordance with a pre-determined schedule. Furthermore, to reduce the burden on utility and Commission staff, utilities will file every three years, with the filing requirements staggered to balance amount of yearly filings received during the

146 *Supra* note 121 at 3-4.
147 *Supra* note 137.
148 *Supra* note 137 at 5.
149 *Supra* note 137 at 5.
150 *Supra* note 137 at 6.
151 *Supra* note 137 at 6.
152 *Supra* note 137 at 4.

three-year period.[153] All Commission-regulated utilities, regardless of number of customers, are required to verbally report "cyber-security breaches that impact IT, OT, or Smart Grid Systems" to the Commission's Chief Engineer within one business day of confirmation.[154]

Importantly, the Commission retained the option of reconstituting the CSRWG to address novel issues or resolve uncertainties generated by operationalizing the briefing process.[155] Having a platform to discuss and resolve issues is essential to creating the flexibility to evolve processes in concert with shifting risk profiles and emerging threats.

TEXAS

Texas has moved to enhance internal information flows between utilities and regulators while protecting confidential information from being publicly disclosed. In 2019, Texas passed three cybersecurity bills[156] including a bill to create an independent cybersecurity monitor.[157] The cybersecurity monitor will oversee cybersecurity efforts among utilities in the state, provide direction on best practices, review voluntary self-assessments, facilitate sharing of information between utilities, and provide guidance for supply chain risk management.[158] Additionally, the monitor will conduct internal cybersecurity risk assessments, vulnerability testing, and employee training[159] and report annually to the Public Utility Commission of Texas on its compliance with applicable laws.[160] Information submitted in the report will be statutorily classified as confidential and exempted from the state public records law.[161]

To facilitate internal information flow, the staff of the cybersecurity monitor is permitted to communicate any cybersecurity information to Commission staff, without exception. Commission staff must maintain the confidentiality of the information and may not disclose it through an open meeting or a response to a public records request, unless subject to another law.[162] This pattern of restricting the number of persons with access to information is a simple way of elevating information security.

Smart Grid Reports

Digitization and automation are increasing the attack surface of the grid. More and more devices are being connected to the grid and grid management is increasingly reliant on virtual management of assets. Thus, it makes sense to consider how processes designed

153 *Supra* note 137 at 5.
154 *Supra* note 137 at 6. Under the prior order, the utilities were required to separately retain and fund an independent cybersecurity consulting firm that would provide annual cybersecurity confidential briefings, to the designated and approved parities, a frequency determined by the Commission. Furthermore, all written materials distributed at the briefing were to be retained by the utilities with the option for the Commission to retain the annual report subject to it meeting specified security measures.
155 *Supra* note 145 at 2.
156 Texas S.B. 475, An act relating to an advisory body on the security of the electric grid (2019); Texas S.B. 64, An act relating to cybersecurity for information resources (2019); Texas S.B. 936, An Act relating to a cybersecurity monitor for certain electric utilities (2019).
157 Texas S.B. 64, An act relating to cybersecurity for information resources (2019).
158 22 Tex. Admin. Code § 31.052(a)(1-2).
159 23 Tex. Admin. Code § 39.151(o)(1).
160 23 Tex. Admin. Code § 39.151(o)(2).
161 23 Tex. Admin. Code § 39.151(p)(2).
162 23 Tex. Admin. Code §39.1516(g).

to evaluate the impacts, effects, and benefits of the increased digitization of the grid or the growing number of distributed energy resources could be adapted to assess a utility's cybersecurity performance. Opportunities exist in the many types of reports that utilities are required to produce. By utilizing existing reporting obligations, utilities and utility commissions gain the advantage of enhanced communication without creating new compliance burdens.

This segment focuses on smart grid implementation reports.[163] While these are the examples selected, the language and reporting requirements could be applied to introduce cybersecurity consideration into reliability reports, distribution system planning reports, distributed energy resource planning reports, or integrated distribution system planning reports. Moreover, the suggestions are intended to be applied to programs already underway or programs in development.

Smart Meters

Smart meter penetration has reached a level where it creates a natural opportunity to address cybersecurity preparedness. The maturation of smart meter implementation programs is an opportunity to reconceptualize the purpose of smart grid reporting to address operational system security. The continued rollout of smart meters creates another opportunity to build in cybersecurity considerations as systems are being built out. Smart meter penetration rates are approaching 50% of U.S. electricity customers. In 2017, U.S. electric utilities had approximately 79 smart metering/advanced metering infrastructure installations[164] with expectations that total installations will reach 90 million by 2020.[165] Furthermore, utilities continue to receive approvals for smart meter programs and to make proposals to develop or expand smart meter programs.[166]

As states complete rollouts, expand existing programs, or evaluate new proposals, cybersecurity reporting requirements should be built into the obligations of utilities. Many states included cybersecurity reporting requirements in their smart meter implementation programs. That was a great start. Those initial requirements often focused on data privacy protection efforts. As awareness of the cyber risk of a connected grid increases, the reporting requirements should shift to examine the cybersecurity preparedness of operations systems. By asking questions that matter, commissions can receive answers that will assist them to evaluate utility performance and decision making.

State Examples

Reports should be more than a snapshot of past practices; they should produce information that can direct future decisions. Oregon and Washington provide examples of

163 Opportunities to build cybersecurity into grid modernization efforts are discussed in Section 6.

164 EIA, Frequently Asked Questions - How many smart meters are installed in the United States, and who has them? October 26, 2018 https://www.eia.gov/tools/faqs/faq.php?id=108&t=3 (retrieved Sept. 9 2019).

165 The Edison Foundation, Institute for Electric Innovation, Electric Company Smart Meter Deployments: Foundation for a Smart Grid (December 2017) https://www.edisonfoundation.net/iei/publications/Documents/IEI_Smart%20Meter%20Report%202017_FINAL.pdf at 2.

166 FERC, Staff Report - 2018 Assessment of Demand Response and Advanced Metering (2018) https://www.ferc.gov/legal/staff-reports/2018/DR-AM-Report2018.pdf at 1.

opportunities of where states could shift the direction and tenor of their smart metering reporting obligations to create an enhanced reporting requirement for cybersecurity preparedness. By tracking each program through its initial development until today, it is apparent that program maturation is an opportunity for renewal rather than a time of senescence.

OREGON

Oregon provides an example of how a commission may respond to the maturation of a smart grid implementation plan to change the objectives of the smart grid reporting program. As implementation programs come to their natural end, the reporting requirements focusing on the build out of the system should shift to investigating the management and protection of operating systems.

Initial Program Development

In 2009, the Public Utility Commission of Oregon opened an investigation to develop smart grid objectives and action items for the next five years.[167] In 2010, Commission Staff presented a straw proposal that included guidelines for smart grid reporting.[168] The Commission found the guidelines to be overly prescriptive and detailed and, instead, ordered the Staff to organize workshops to develop new guidelines, including guidelines for cybersecurity issues.[169] In 2012, the Commission published a list of policy goals and objectives and formalized the structure for the annual reporting requirement.[170]

Cybersecurity was identified in the policy goals and objectives and the mandated contents of the annual reports identified cybersecurity. Both the objectives and the mandated content are reflective of the time in which they were developed and the concern about cyber threats. The Commission wrote that its goal was to "benefit the ratepayers of Oregon investor-owned utilities by fostering investment in … smart-grid measures that are cost-effective to consumers and that achieve some of the following:"[171] Among the options presented was to "[i]ncrease resiliency to withstand physical and cyber attacks, and natural disasters; …"[172] Reporting focused on the construction of the smart grid. Utilities were required to report on smart grid investment plans, provide status updates on ongoing projects and initiatives, and identify key technologies.[173] Discussions on smart grid opportunities and constraints were expected to cover "related activities to address physical- and cyber- security, privacy, customer outreach and education, and IT and communication infrastructure, as they relate to smart-grid activities."[174]

167 Oregon Public Utility Commission, UM 1460, Staff recommendation to open a docket and use Oregon Electricity Regulators Assistance Project funds from the American Recovery and Reinvestment Act of 2009 to develop Commission smart grid objectives and action items for the 2010-2014 time period, December 8, 2009.

168 Oregon Public Utility Commission, UM 1460, Straw Proposal for Utility Smart Grid Planning, October 22, 2010.

169 Oregon Public Utility Commission, UM 1460, Order 11-172, Staff Recommendation to Use Oregon Electricity Regulators Assistance Project Funds from the American Recovery and Reinvestment Act of 2009 to Develop Commission Smart Grid Objectives for 2010-2014, May 25, 2011 at 2, 3.

170 Oregon Public Utility Commission, UM 1460, Order 12-158, Staff Recommendation to Use Oregon Electricity Regulators Assistance Project Funds from the American Recovery and Reinvestment Act of 2009 to Develop Commission Smart Grid Objectives for 2010-2014, May 8, 2012.

171 *Id.* at 3.

172 *Id.* at 3.

173 *Id.* at 5-6.

174 *Id.* at 6.

Changing Reporting Requirements

In 2017, the Commission amended its order to shift to a biannual smart grid report filing requirement. The filing period was altered to provide utilities more time to develop the depth of their answers.[175] However, the Commission did not amend its guidance on the contents of the report and the reporting requirements remain very general as compared to Michigan or Maryland. The requirement that reports be presented at public meeting remains as does the opportunity for the public and Staff to provide for written and oral comments from public and Staff.[176] The option for the Commission to require a utility to address proposed recommendations from the Staff and the public in subsequent reports remains and could be leveraged in the future to enhance information sharing.[177]

As smart grid programs mature, changes to reporting structures should evolve in concert. The maturation of the program creates an opportunity to revise procedural obligations and to revisit the substantive elements of the report. Oregon has in place the objectives to drive the change without requiring a new order from the Commission. Commissions have more knowledge of and greater access to resources on cybersecurity at the end of a smart grid program than the beginning. Applying that knowledge can direct a utility to improve the volume, quality, and depth of their answers, which can lead to action to increase grid resilience to cyber attacks.

WASHINGTON

Washington is another example of how opportunities may present to re-task smart grid reporting requirements to increase attention placed on a utility's cybersecurity posture.

Initial Program Development

Like other states, Washington began its smart meter implementation program after receiving federal funding from the American Recovery and Reinvestment Act.[178] In 2009, the Washington Utilities and Transportation Commission opened an investigation and passed rules, which were adopted into the Washington Administrative Code, setting out the filing schedule and detailing the minimum contents of its smart grid reporting process.[179] The rules required investor-owned utilities to annually file reports to the Commission on their evaluation of smart grid technologies that are available or likely to be available soon and any plans for implementing smart grid technology.[180]

The scope of the reports was comprehensive with a strong focus on managing costs and benefits. The factors selected for reporting represent what information the Commission

175 Oregon Public Utility Commission, UM 1460, Order 17-290, Smart Grid Objectives, July 27, 2017 at 1.
176 Oregon Public Utility Commission, UM 1460, Order 12-158, May 8, 2012 at 4.
177 *Id.*
178 U.S. Department of Energy, The American Recovery and Reinvestment Act: Smart Grid Highlights, October 2014, https://www.energy.gov/sites/prod/files/2014/12/f19/SGIG-SGDP-Highlights-October2014.pdf at 4.
179 Washington Utilities and Transportation Commission, Docket U-090222, General Order R-559, Order Adopting Rule Permanently, In the Matter Adopting WAC 480-100-505 Smart grid technology report, Relating to the Review of the PURPA Standards in the Energy Independence and Security Act of 2007, March 24, 2010.
180 Wash. Admin. Code § 480-100-505(1) (2010).

needed during the smart grid development and implementation phase to evaluate utility planning processes and technology procurement proposals. Cybersecurity considerations, for operations system and information systems, were included. Overall, the utilities were expected to provide details on technologies that the utility has considered and evaluated including:

> (i) *Goal or purpose of the smart grid technologies described in the report;*
>
> (ii) *Total costs of the deployment and use of smart grid technologies including meter or other equipment costs, installation costs, and any incremental administration costs including the cost of changes to data storage, processing and billing systems;*
>
> (iii) *Overall cost-effectiveness of smart grid technologies planned to be implemented and, to the extent it can be quantified, possible impacts on customer bills;*
>
> (iv) *Operational savings associated with meter reading or other utility functions;*
>
> (v) *Effects on system capability to meet or modify energy or peak loads;*
>
> (vi) *Effects on service reliability including storm damage response and recovery, outage frequency and duration and voltage quality;*
>
> (vii) *Effects on integration of new utility loads, such as recharging batteries in electrically powered vehicles;*
>
> (viii) *Cyber and physical security of utility operational information;*
>
> (ix) *Cyber and physical security of customer information and effects, if any, on existing consumer protection policies;*
>
> (x) *Interoperability and upgradability of technology and compliance with applicable national standards;*
>
> (xi) *Customer acceptance and behavioral response;*
>
> (xii) *Tariff and rate design changes necessary to implement the technology;*
>
> (xiii) *Nonquantifiable societal benefits, if any; and*
>
> (xiv) *Economic considerations recognizing the above-listed factors.*[181]

The reporting obligations ceased in 2016 as utilities completed their smart meter implementation programs.[182] Smart meter program maturity does not negate the need for continued information exchange and in fact it could provide an opportunity to revise filing requirement to focus on system performance and security. The conclusion of smart metering program reporting obligations does not have to follow the completion of a utility's smart meter implementation program and it did not in Washington.

Changing Reporting Requirements

In 2018, the Commission opened a docket to begin the process of modifying the "existing consumer protection and meter-related rules to accommodate regulated utility deployment

181 Wash. Admin. Code § 480-100-505 (2010).
182 Wash. Admin. Code § 480-100-505(3)(b) (2010).

of Advanced Metering Infrastructure (AMI) technologies."[183] The proceeding is focused on customer choice data access and data privacy, but it could as easily been tailored to enhance utility reporting on cybersecurity practices and protocols.

The ability to revise reporting requirements to address emerging issues and concerns is a power held by every utility commission. A reporting system designed a decade ago reflects the prevalent issues and concerns of that time. Amending the content requirements, extending the reporting obligations, and altering the reporting methodology are all options for commissions seeking to advance their understanding of how the utilities are responding to the changing cyber threat matrix.

Management and Operations Audits

Management and operations audits[184] are tools that can be deployed to assess company performance, identify gaps in regulatory oversight, and gather information for the promulgation of formal rules. Which is what makes them ideal for assessing cybersecurity preparedness.

All commissions possess the power to audit utility operations for performance and efficiency. Management audits are a common practice with commissions from Maine[185] to Mississippi[186] holding the authority to order an audit of a regulated utility. Management audits are an established part of utility commission practice. In 1979, NRRI documented the rise in use of commission-ordered management audits and the value offered by the external review of utility operations.[187] Recently, management audits have been used to evaluate the state of cybersecurity preparedness and the effectiveness of management decisions and utility investments.

The reason why management audits are useful in assessing a utility's cybersecurity preparedness lies in the flexibility of their design. Management audits allow commissions to focus in on specific areas of utility operations and assess a utility's performance. Management audits can assess the performance of a single utility, a group of utilities, or all utilities. The freedom to design and initiate an audit ensures that audits happen in a timely manner to produce a report that informs key decisions. The audits can be conducted by commission staff or by an independent party third-party, which enables the commission to make optimize available resources and expertise. Importantly, whether conducted in-house or by outside experts, a management audit boosts the institutional knowledge of regulatory staff by providing insight into utility operations and decision-making processes.

An audit should serve review of past practices and outline future improvements. The results of a management audit can assist a utility commission in determining where performance is lagging or leading and how to address concerns. The results from an audit of a single utility can be used to elevate practices amongst all utilities. The results of a group audit can assist in determining whether additional rulemaking is needed.

183 Washington Utilities and Transportation Commission, Notice of Opportunity to File Written Comments (By September 7, 2018), Re: Rulemaking to modify existing consumer protection and meter rules to include Advanced Metering Infrastructure, Docket U-180525 (July 10, 2018) at 1.

184 Management audits differ from financial audits. While financial audits are often a part of rate case proceeding where a utility has requested a rate increase, management and operations audits focus on utility operations and performance.

185 Me. Rev. Stat. 35-A 113.

186 Miss. Code Ann. § 77-3-46.

187 The National Regulatory Research Institute, Commission Ordered Management Audits of Gas and Electric Utilities, July 1979 http://ipu.msu.edu/wp-content/uploads/2016/12/NRRI-Gas-Electric-Audits-79-11-July-79-1.pdf.

Many statutes and regulations creating audit authority focus on utility construction practices and ensuring the prudent investment of ratepayer funds. While broad language like Mississippi's empowerment of its utility commission to examine the "efficiency and effectiveness of management decisions" [188] is preferable, narrowly tailored statutory or regulatory provisions should not be a barrier to conducting comprehensive investigations into cybersecurity preparedness. Cybersecurity can and should be included in any construction management audits going forward. It is easily argued that utilities should be proactively considering the effectiveness of cybersecurity infrastructure investments, as evidenced by the Massachusetts example.

Lastly, the processes of conducting the audit and presenting the results must balance the vulnerability held within the results against the value of public discussions. Commissions should attempt to publish the results of the audits, with redactions as necessary for confidential information.

State Examples

The following state examples present exemplars of how management and operations audits can build in cybersecurity considerations. Management and operations audits should look backward and project forward. They can assess individual decision-making and overall utility culture. The utility commissions highlighted in this section have used their audit powers to assess cybersecurity protections and move their regulated utilities towards a best practices approach to risk management.

FLORIDA

One of the best examples of how a management audit can be employed to evaluate cybersecurity practices is the use of the audit power by the Florida Public Service Commission. The Commission has a dedicated office, the Office of Audits and Performance Analysis, tasked with auditing Florida's utilities.[189] The Office exercised its authority twice in the past five years to evaluate the physical security and cybersecurity posture of Florida's investor owned utilities.[190]

The authority given to the Public Service Commission to conduct management and operations audits of regulated utilities is comprehensive. The Commission is empowered to conduct such audits as it deems necessary without a restriction on the number of audits or the period between audits.[191] Auditors are granted access to utility and utility

188 Miss. Code Ann. § 77-3-46.

189 Florida Public Service Commission, Statement of Agency Organization & Operations, January 2019 http://www.psc.state.fl.us/Files/PDF/Home/SAOO.pdf at 8.

190 In 2014, the Office of Audits and Performance Analysis completed and published the "Review of Physical Security Protection of Utility Substations and Control Centers" which was followed by 2018's "Review of Cyber and Physical Security Protection of Utility Substations and Control Centers." Florida Public Service Commission, Office of Auditing and Performance Analysis, Review of Physical Security Protection of Utility Substations and Control Centers, December 2014, http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf; 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, http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf.

191 Fl. Stat. § 350.117 (2006).

affiliate records with an expansive definition of what is relevant to the audit.[192] The "audit scope, audit program and objectives, and audit requests are not constrained by relevancy standards narrower"[193] than those Commission staff are entitled, by statute, for accessing records of transactions or cost allocations when conducting financial audits.[194] Moreover, reasonable access to records includes "reasonable access to personnel to obtain testimonial evidence in response to inquiries or through interviews"[195] which allows Commission staff to interview key utility personnel.

How the audit power is deployed is an important design choice that can magnify potential benefits. For example, in 2014 and 2018, the Office simultaneously audited all the investor-owned utilities on their cybersecurity practices and protocols, thus allowing for a comparison of operational practices and the exchange of information on best practices.

NEW YORK

A recent example from New York illustrates the type of information a management audit can provide when the Commission and the Department of Public Service exercise their authority to the scope of the shape of the audit. Under New York law, each regulated gas and/or electric utility is subject to a management and operations audit. For combination gas and electric utilities or gas utilities with annual gross revenues in excess of 200 million dollars, audits are to be performed at least once every five years.[196] The scope of the audits are broad. An audit must, but is not limited to, investigate the utility's construction program in relation to providing reliable service, evaluate the efficiency of the utility's operations, and produce recommendations for each along with a timeline for implementing the recommendations.[197] The Public Service Commission also retains the right to determine whether the audits will be performed by Commission staff or by an independent auditor.[198]

In 2016, the Commission issued a request for proposals to audit two large electric and gas utilities, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation.[199] The RFP set out seven elements of the audit which were further broken down into multiple components.[200] Under the Corporate Governance element, bidders were required to set forth how they would assess the enterprise risk management program of the utilities.[201] Under the Electric Planning and REV Preparations, bidders were required to "identify, describe, and evaluate the utilities' electric supply portfolio principles, objectives, policies, processes, oversight, and risk management strategies."[202]

The bid accepted by the Commission was the only bid that specifically listed cybersecurity

192 Fla. Admin. Code Ann. r.25-6.0151 (1995).
193 Fla. Admin. Code Ann. r.25-6.0151(1) (1995).
194 Fl. Stat. § 366.093 (1989).
195 Fla. Admin. Code Ann. r.25-6.0151(5) (1995).
196 NY Pub Serv Law § 66(19)(a).
197 *Id.*
198 *Id.*
199 New York Public Service Commission, Request for Proposals to Perform Comprehensive Management and Operations Audits of New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation, Case 16-M-0610, December 15, 2016.
200 *Id.* at 12-13.
201 *Id.* at 13.
202 *Id.* at 14.

as an issue in the evaluation of the utilities' risk management programs and priorities. The selected bidder described how it would review the utilities' risk program, if it had one, for identifying and mitigating specific risks associated with the Renewing the Energy Vision docket and cybersecurity.[203] Furthermore, the audit would also examine processes for managing cyber breaches.[204]

The audit report is an opportunity to identify good practices and places for improvement. In the final audit report, some gaps were identified although the parent utility was commended for good cybersecurity risk management practices. The auditors recommended that the parent utility institute core cybersecurity compliance metrics to evaluate the effectiveness its cybersecurity program.[205] The utility, in its response, has provided a timeline for implementing the recommendations and has been providing implementation updates.[206]

Note: New York's cybersecurity-specific audits are conducted on a quarterly basis by Commission staff. More information on the structure of the audits can be found in Section 4 of the Phase 1 Report.[207]

MASSACHUSETTS

On September 30, 2019, Massachusetts initiated a management audit for National Grid that will examine several issues including cybersecurity investments. Under Massachusetts law, the Department of Public Utilities is given the broad authority of "general supervision of all gas and electric companies" and the power to audit the utilities to ensure that property and practices of the utility are maintained and conducted in accordance with state law, commission orders, and commission directives.[208]

The audit arose out of National Grid's most recent general rate case filing. During the proceeding, the Department and the Attorney General expressed concerns on whether National Grid's "IT strategy and cybersecurity plan focus appropriately on benefits to Massachusetts ratepayers."[209] The Department found some merit in the Attorney General's argument that National Grid's approach to "IT investments is reactive, uncoordinated, and has not been vetted to determine benefits Massachusetts ratepayers receive for the costs allocated to them."[210] Based on those concerns, and general concerns over management practices, the Department opened a docket, and began accepting comments from stakeholders, to determine the final scope of the audit procedures.[211]

203 Overland Consulting, Proposal to Perform Comprehensive Management and Operations Audits of New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation, Case 16-M-0610, February 9, 2017 at 2-8.
204 *Id.* at 2-17.
205 Overland Consulting, Comprehensive Management and Operations Audits of New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation, Case 16-M-0610, November 2018 at 6.14-15.
206 NYSEG and RG&E, NY Management Audit Implementation Plan Update, July 19, 2019.
207 *Supra* note 1 at 24.
208 Mass. Gen. Laws ch. 164, §76.
209 Massachusetts Department of Public Utilities, D.P.U. 18-150, Petition of Massachusetts Electric Company and Nantucket Electric Company, each doing business as National Grid, pursuant to G.L. c. 164, § 94 and 220 CMR 5.00, for Approval of General Increases in Base Distribution Rates for Electric Service, September 30, 2019 at 499.
210 *Id.*
211 *Id.*

Conclusion

Reporting requirements and audit processes are an underutilized opportunity to assess the cybersecurity posture of individual utilities or to make a broader assessment of the cybersecurity activities of the entire sector. Utility commissions have tremendous powers of oversight. As the grid evolves, the traditional reporting and auditing practices should follow along. The information generated from these processes can play an outsized role in elevating the knowledge of the commission and preparing utilities for the challenge of protecting their systems. Furthermore, the processes for collecting information from utilities are well-trodden and can be repurposed within only minor changes in their scope, goals, and objectives. Deploying these tested practices for cybersecurity purposes is a simple step that any commission can take to gain insight into a utility's cybersecurity management and operation practices.

SECTION 4

COST RECOVERY MECHANISMS

PROTECTING THE GRID AGAINST A CYBERATTACK will require substantive investments in technology and people. The need for investment is an acknowledged fact[212] as is the fact that security and resiliency improvements follow investment in new technology and additional staff and training. What is debated is the best way to create conditions for that investment. The Phase 1 Report identified and explored the issue of what is needed to ensure appropriate levels of investment are being made to enhance and upgrade distribution utility cybersecurity protections. In several interviews, the question of regulatory lag was raised given the shorter lifespan of cybersecurity investments compared to traditional utility investments. Alternative rate mechanisms, mechanisms that allow for more expeditious cost recovery outside of a general rate case proceeding,[213] were proposed as a potential solution. As utilities increasingly propose the use of alternative rate mechanisms to incentivize cybersecurity investments, legislatures and commissions will need a balanced approach to weigh the benefits of the alternative rate mechanism against its potential shortcomings, such as a reduction in formal due process and public scrutiny. This section present options for designing alternative cost recovery mechanisms that can incentivize cybersecurity investments while protecting the public interest.

212 Ponemon Institute and Siemens, Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat? Assessing Operational Readiness of the Global Utilities Sector, October 2019 at 15.

213 General rate case is the term employed in this report to describe the traditional cost of service ratemaking process. Base rate case will occasionally be used in the report as this term is often used interchangeably with general rate case.

Investment Needs

The legacy grid operating today is the compilation of decades of development, investment, and inertia. The grid was built out over multiple decades as utilities expanded or emerged to serve new areas and territories. Investment in making the grid more reliable, more efficient, and more secure have bolted new equipment and processes onto decades-old decisions. The already patchwork nature of the grid will be subject to even more modification as new digital technologies for managing system operations and dispatch are adopted. As new digital systems connect, the attack surface of the grid grows and the need for additional investment in cybersecurity mounts. Investment is needed to upgrade the existing security posture of the grid and to prepare the grid for millions of soon-to-be connected distributed energy resources and other networked devices.[214]

Cybersecurity Investment

Currently, cybersecurity investments are a small portion of overall utility investments relative to overall utility investments in infrastructure and operations. However, they are a growing percentage of investments as utilities ramp up spending on grid modernization and they are an ever-present concern for utility regulators worried about the potential costs of not being prepared for a cyber attack.

Utilities are now investing in cybersecurity. In the past year, the Rhode Island Public Utilities Commission approved recovery by National Grid of almost $5 million in operations and maintenance and infrastructure cybersecurity investments;[215] the Virginia State Corporation Commission approved Dominion Energy's investment of $35.2 million dollars in cyber and physical security over a three-year period;[216] Ameren Missouri proposed an investment of $448 million dollars in technology and cybersecurity as part of its five-year capital investment program;[217] and Duke Energy put forth a six-state proposal for cybersecurity investments.[218] These examples build on the past decade of cybersecurity investments[219] and represent a small selection of states where distribution utilities are investing in cybersecurity.

214 Ridge Global, Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors: A Risk Assessment Study of Solar Inverter Technology, October 29, 2019 https://protectourpower.org/wp-content/uploads/2018/11/Ridge-Global-and-Potential-Electric-Grid-Vulnerability.pdf; Jason Deign, Green Tech Media, Inspection Firm Hacks Inverters Within Minutes, Casting Doubt on Security, May 23, 2018 https://www.greentechmedia.com/articles/read/tuv-hack-inverter-security#gs.ws3dvg; https://arxiv.org/pdf/1907.08283.pdf; Blake Sobczak, EnergyWire, Hacked EV chargers could cause blackouts – study, August 19, 2019 https://www.eenews.net/energywire/2019/08/19/stories/1060995703.

215 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.

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

217 Ameren Missouri, Ameren Missouri 5-Year Electric Customer-Focused Capital Investment Plan, Exhibit 1, 2019 https://www.efis.psc.mo.gov/mpsc/commoncomponents/viewdocument.asp?DocId=936206048.

218 Duke Energy, Letter to FERC, Re: Duke Energy Corporation, Docket No. Ac19- -000 Accounting Request Related to Cybersecurity Informational Technology-Operational Technology Program, March 13, 2019 at 2.

219 Daniel Phelan, NRRI, A Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues (2014) at 11-15.

The total amount of investment is forecasted to nearly double in the next decade[220] as more state commissions open grid modernization dockets and begin the process of encouraging cybersecurity programs. In the second quarter of 2019, 33 states made 116 legislative or regulatory actions addressing grid modernization polices, 32 states and territories took 75 legislative or regulatory actions addressing grid modernization deployment, and 31 states and territories took legislative or regulatory actions addressing grid modernization studies or investigations.[221] As the transformation unfolds, the issue that keeps cropping up is whether the historic cost recovery mechanisms adequately incentivize the levels of investment required to boost the resiliency of the grid.

Cybersecurity and Regulatory Lag

Regulatory lag was raised as a concern in Phase 1 of our cybersecurity research. Utilities expressed concern that rapidly increasing cybersecurity investment needs would put pressure on their business models and that the resulting regulatory lag may negatively influence decisions when to invest in security measures. Similar concerns were raised at the March 2019 FERC/DOE Technical Conference, "Security Investments for Energy Infrastructure."[222] The changing nature of the electricity business model magnifies these concerns now and in the future. Flat or declining load growth is the new norm for most distribution utilities[223] and that new norm will have an impact on utility investment patterns. Magnifying this concern is that an investment in cybersecurity is in important ways different than a traditional utility investment, further threatening the historic utility business model.

Cybersecurity investments are a different type of utility investment that a traditional utility investment in infrastructure. Cybersecurity investments have shorter lifespans in the range of 3-7 years instead of the 30 to 40-year lifespan of poles and wires. Investment is needed in a combination of software, hardware, and training which all have different characteristics and rate treatments. A compounding factor is that the risk of redundancy is greater because of the rate of change in technologies and the pace at which threats emerge and are identified. Adding to the risk element is that cybersecurity protections are less likely to produce offsetting revenue increases or expense reductions, although they might be paired with other technology that does.

220 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.

221 Autumn Proudlove et. al, North Carolina Clean Energy Technology Center, 50 States of Grid Modernization, Q2 2019 Quarterly Report – Executive Summary, July 2019, https://nccleantech.ncsu.edu/wp-content/uploads/2019/07/Q22019_gridmod_exec_final.pdf at 6.

222 FERC/DOE Security Investments for Energy Infrastructure, Technical Conference, Docket No. AD19-12-000, March 28, 2019, Transcript at 78, 139-140, 152, 200-201. https://www.ferc.gov/CalendarFiles/20190426140022-Transcript%20032819FERC_DOESecurity.pdf.

223 Energy Information Administration, Annual Energy Outlook 2017, Table: Electricity Supply, Disposition, Prices, and Emissions (2017) https://www.eia.gov/outlooks/aeo/data/browser/#/?id=8-AEO2017&region=0-0&cases=ref2017&start=2015&end=2050&f=A&linechart=~ref2017-d120816a.56-8-AEO2017&map=&ctype=linechart&sourcekey=0.

DEFINING REGULATORY LAG

Regulatory lag is the length of time between when additional costs occur and when the new revenue are recovered in rates.[224] Utilities incur costs through both capital expenditures and operational and maintenance expenditures.[225] Those prudently incurred costs are recovered from ratepayers through monthly billing cycles. Costs are recovered after regulators have approved the utility's costs of doing business and allowed them into the annual revenue requirement which is translated into customer rates. As costs increase or new costs occur, a gap between the time the cost is incurred and the time the approved revenue is recovered in rates may develop. That gap is regulatory lag.

Regulatory lag is the natural product of a rate regulated industry. While regulatory lag can negatively impact a utility's bottom line, it can also incentivize regulated utilities to pursue efficiencies and innovation since cost savings can increase short-term profits or offset other rising costs. When costs are increasing regulatory lag incentivizes utilities to file frequent rate cases to recover the increasing costs. Frequent rate cases are time consuming and can be very costly to utilities, public utility commissions, intervenors, and ultimately ratepayers. While full rate cases may provide increased due process and transparency, it is an expensive process that may also discourage intervenor participation. The investment of time and resources into completing a rate case has encouraged utilities and regulatory commissions to seek more efficient alternatives.

Regulatory lag should not be fully viewed in black and white terms as either a positive or negative aspect of utility regulation. It can negatively affect utility decisions on when to and how to invest in critical infrastructure, a decision that becomes more tenuous in times of declining or flatlining load growth. If costs increase when electric sales are flat or decreasing, the financial position of the utility will be impacted.[226] During period when many utilities are facing declining or flatlining load growth,[227] regulatory lag can become a significant disincentive for new investments that provide benefits unrelated to increased sales. Under this likely scenario, regulatory lag can affect utility infrastructure investment decisions of whether to invest, how much to invest, and when to invest. Overall, the level of financial impact is tied to the full utility cost and revenue situation and should be evaluated within the context of all utility revenue streams.

The impact of regulatory lag on investment is likely to be elevated for investment in non-revenue generating infrastructure and capital expenditures (safety, reliability, and resilience).[228] Therefore, regulators must consider the value of other policy objectives when assessing the economic impact of lower investment in non-revenue generating infrastructure, particularly infrastructure that is directly connected to the security and reliability of the grid. The question at hand is what are the goals that the regulators and system operators seek to pursue and does the current system construction allow for utilities to do that and be rewarded for investing in those areas.

224 Jim Lazar et al., Regulatory Assistance Project, Electricity Regulation in the US: A Guide, Second Edition (2016) at 195.
225 James C. Bonbright et al., Principles of Public Utility Rates, 2nd Edition, Public Utilities Reports, Inc., (1988).
226 *Supra* note 224 at 88.
227 Energy Information Administration, Annual Energy Outlook 2017, Table: Electricity Supply, Disposition, Prices, and Emissions (2017) https://www.eia.gov/outlooks/aeo/data/browser/#/?id=8-AEO2017&region=0-0&cases=ref2017&start=2015&end=2050&f=A&linechart=~ref2017-d120816a.56-8-AEO2017&map=&ctype=linechart&sourcekey=0.
228 Ken Costello, NRRI, Alternative Rate Mechanisms and Their Compatibility with State Utility Commission Objectives (2014) at 16.

The effect of regulatory lag on cybersecurity investments is modest right now.[229] Projecting forward, cybersecurity investment needs will grow exponentially in both value and as a portion of overall investments. Consequently, the impact of regulatory lag will grow too. The digitization and diversification of the grid means that millions of new devices will be connecting to the grid in coming decades and each of those connections will increase the attack surface of the grid. Since most of those connections will occur on the distribution grid, distribution utilities will weigh their options for investing in new cybersecurity technology, staff, and training. Now is the perfect time to discuss the need for alternative rate mechanisms and options for deploying them to be prepared for the coming changes. It is also the time to discuss how to deploy them to ensure that the public interest is protected.

ALTERNATE RATE MECHANISMS

An alternative rate mechanism is a mechanism that allows for cost recovery outside of a general rate case proceeding.[230] A general rate case proceeding is a contested process where the regulator reviews all costs, the allowed return, the revenue requirement of the utility, and any challenged items. The general rate case provides predictability and stability in rates and a platform for stakeholders to present their arguments on what is fair, just, and reasonable rate.[231] Alternative rate mechanisms operate outside of the general rate case process and may not provide the same opportunity for due process, stakeholder participation, and transparency.

Traditional ratemaking has incorporated alternative rate mechanisms to achieve different objectives such as reducing the frequency of rate cases, reducing the risk from large and unexpected costs, and allowing for investment in specific projects with defined goals.[232] However, the dominant method for determining whether a utility can recover its prudent costs remains the general rate case, even for cybersecurity investments.[233] While the interest in alternative rate mechanisms has grown, there is not a consensus in favor of these mechanisms. . There is a strong belief that alternative rate mechanisms should be used only "when market, economic, operating, technological, and other conditions change."[234]

Alternative rate mechanisms come in a variety of forms including decoupling, adjustment mechanisms, infrastructure trackers and riders, future test years, and deferred accounting

229 Phase 1 report interviewees and the presenters at the March 28th FERC Technical Conference were in alignment on the current and future levels of pressure caused by regulatory lag. *Supra* note 1 at 41; *Supra* note 222 at 200.

230 *Supra* note 224 at 100. General rate case is the term employed in this report to describe the traditional cost of service ratemaking process. Base rate case will occasionally be used in the report as this term is often used interchangeable with general rate case.

231 *Id.* at 40.

232 *Supra* note 228 at 1.

233 I. Pena, M. Ingram, and M. Martin, NREL, States of Cybersecurity: Electricity Distribution System Discussions (2017) at 28. This finding was confirmed in the interviews conducted for the Phase 1 report.

234 *Supra* note 228 at 12 citing Paul L. Joskow, "Inflation and Environmental Concern: Structural Changes in the Process of Public Utility Regulation"; Karl McDermott, Cost of Service Regulation in the Investor-Owned Electric Utility Industry: A History of Adaptation (Washington D.C.: Edison Electric Institute, June 2102); and Kenneth W. Costello and Douglas N. Jones, "Lessons Learned in State Electric Utility Regulation," in Reinventing Electric Utility Regulation, eds. Gregory B. Enholm and J. Robert Malko (Vienna,VA: Public Utilities Report, 1995) at 69-92.

mechanisms.[235] The section focuses on the use of cost riders or trackers. Based on our Phase 1 research, cost riders were the most commonly proposed option for recovering the new investment costs. Thus, we focus on that option, although the questions could be expanded to address the impact of any proposed alternative rate mechanism.

A cost rider or a tracker is an adjustment mechanism used to recover a specific "cost, revenue, tax, or other element of utility rates" is recovered without waiting for a general rate case proceeding.[236] Cost riders are deployed in between rates cases to reduce regulatory lag by expediting cost recovery.[237] Cost riders are usually single-issue adjustment mechanisms focusing on one aspect of a cost change.[238] For example, cost riders have been deployed to recover new investments in transmission and distribution system infrastructure, decommissioning costs, or to for fuel costs.[239] The alternative rate mechanism examples presented in this section are almost entirely composed of distribution system cost riders.

This section presents a series of questions that guide the decision of whether to deploy an alternative rate mechanism and how to design the alternative rate mechanism to achieve regulatory objectives and goals. Examples of state statutes, commission regulations, and commission orders are presented to demonstrate how other states have answered these questions.

QUESTION #1:
DOES THE COMMISSION HAVE THE AUTHORITY TO DEPLOY AN ALTERNATIVE RATE MECHANISM?

Before a utility can request recovery of its investment costs via an alternative rate mechanism, the Commission must have the authority to grant recovery via an alternative rate mechanism. Specifically, is there legislation that defines the parameters of what types of utilities can request the use of the rate mechanism and what procedural steps must be followed. There are two essential conditions: the cost recovery mechanism must be available to electric utilities and it must permit recovery of distribution system investments.

In recent years, several states have enacted legislation granting the authority for utilities to request cost recovery for investments in their systems or for investments in specific types of projects. In Texas, the state legislature created the Distribution Cost Recovery Factor (DCRF) to allow for recovery of capital investments in distribution infrastructure.[240] The DCRF mirrored an existing cost recovery mechanism for investment in transmission system infrastructure. Interestingly, the Texas legislature created the DCRF, but it was the Public Utility Commission of Texas that initially proposed the rule before deferring to the Legislature to weigh in.[241] In 2018, Virginia passed the Grid Transformation and

235 This list is not conclusive and represents some of the most common forms of alternative rate mechanisms.
236 *Supra* note 224 at 103.
237 Johnathan Lesser and Leonardo Giacchino, Fundamentals of Energy Regulation (2013) at 270.
238 *Id.*
239 *Supra* note 224 at 103.
240 16 Tex. Admin. Code § 25.243(c)(1)(C).
241 Public Utility Commission of Texas, Report to the 82nd Texas Legislature, Scope of Competition in Electric Market in Texas (2011) at 11.

Security Act which created a cost recovery mechanism for qualifying projects.[242] In 2015, Minnesota amended its law to allow for distribution system investments to be recovered under a cost recovery mechanism originally designed to incentivize transmission system investments.[243]

The need for an alternative rate mechanism is a question that can be answered by a utility commission. Commissions should be empowered to be proactive, not just reactive to requests for new recovery mechanisms. Commissions can take the initiative and control the process by identifying the principles and objectives that it will use to determine the need for an alternative rate mechanism.[244] This process can work to identify the need for alternative rate mechanisms or the lack of supporting evidence for the conditions that necessitate alternative rate mechanisms.

In 2016, the Missouri Public Service Commission opened a docket to gather information and stakeholder input on how the Commission regulated Missouri's investor owned utilities.[245] The Staff Report discussed, at length, the question of regulatory lag and its impacts on investment decisions and patterns.[246] In its final order, the Commission produced a set of four principles that the General Assembly should consider if it drafted any legislative proposal. The four principles were: avoid massive, radical overhaul; any new mechanism should not impede the Commission's authority or ability to meet its statutory obligation of just and reasonable rates while balancing utility and customer interests; any modification of the regulatory structure should be narrowly tailored; and any utility's use of a new rate mechanism should be contingent upon Commission review and authorization.[247] Those principles would serve any commission considering whether to authorize the use of an alternative rate mechanism.

QUESTION #2:
IS THE ALTERNATIVE RATE MECHANISM NECESSARY?

Ratemaking Principles

After acknowledging the existence of the desired alternative rate mechanism, the next question is whether its deployment respects the balance between the public interest and the interests of the company. If the use of the mechanism unreasonably shifts risk from shareholder to ratepayer, it raises legitimate questions about the decision to utilize the mechanism. Those questions do not preclude or prevent the deployment, they instead require legislators and regulators to examine how the balance might be restored through different accommodations, as is discussed below.

242 Virginia, S.B. 966, Grid Transformation and Security Act of 2018.
243 Minnesota, Jobs and Economic Development Appropriations Act (2015) amending MN ST § 216B.16 (Subd. 7b)(i).
244 *Supra* note 228 at 18.
245 Missouri Public Service Commission, File No. EW-2016-0313, Order, In the Matter of a Working Case to Consider Policies to Improve Electric Utility Regulation, June 8, 2016.
246 Missouri Public Service Commission, File No. EW-2016-0313, Staff Report, A Working Case to Consider Policies to Improve Electric Utility Regulation, October 17, 2016 at 18.
247 Missouri Public Service Commission, File No. EW-2016-0313, In the Matter of a Working Case to Consider Policies to Improve Electric Utility Regulation, December 6, 2016 at 3-6.

The argument that a company is not earning its regulated rate of return and is therefore deserving of an alternative rate mechanism is not determinative of the question whether to deploy the mechanism. The argument is complex and requires the commission to study the overall impact of the actual return on investment on future investment prospects. A utility has the opportunity to earn its regulated rate of return not the right to earn its regulated rate of return. And as noted above, regulatory lag is an accepted part of utility regulation and can serve a beneficial purpose.

Commissions should "consider the merits of alternative rate mechanisms when market, economic, operating, technological, and other conditions change."[248] For example, a federal or state law requiring investment in grid modernization and cybersecurity would be an example of a trigger that would require the commission to consider the validity of its current ratemaking structure. Another change could be the emergence of new and persistent threats or the exposure of systemic vulnerabilities that could compromise operational integrity.

Adding to the complexity of this evaluation is the unique characteristics of cybersecurity investments. Cybersecurity investments have shorter lifespans due to the pace of change in technology. A five to seven-year lifespan for a hardware or software component is much shorter than that of a pole, line, or transformer. Cybersecurity protections require investment in hardware, software, and personnel. Determining where resources are most needed is like playing a game where the rules constantly change. Utility risk profiles are constantly evolving with the identification of new threats and vulnerabilities, which means that investment priorities may change.

Demonstrating Need

In all cases, the burden of demonstrating need should be shifted onto the utility and states can and should evaluate the financial reasoning for requesting the alternative rate mechanism. The burden of proof should be substantial and involve the utility demonstrating that a significant change has occurred, or a significant need has arisen that cannot sufficiently be met through traditional rate recovery in a general rate case proceeding. There are multiple ways of requiring utilities to demonstrate financial need as the following examples illustrate.

In Texas, utilities must file an earnings monitoring report for the immediately proceeding calendar year.[249] A utility will be denied permission if the earnings monitor report shows that the electric utility is "earning more than its authorized rate of return using weather-normalized data."[250]

In Ohio, the Public Utility Commission had an extensive evaluation of a proposal to create a grid modernization rider. The Commission, in granting the use of a distribution

248 *Supra* note 228 at 12 citing Paul L. Joskow, "Inflation and Environmental Concern: Structural Changes in the Process of Public Utility Regulation"; Karl McDermott, Cost of Service Regulation in the Investor-Owned Electric Utility Industry: A History of Adaptation (Washington D.C.: Edison Electric Institute, June 2102); and Kenneth W. Costello and Douglas N. Jones, "Lessons Learned in State Electric Utility Regulation," in Reinventing Electric Utility Regulation, eds. Gregory B. Enholm and J. Robert Malko (Vienna, VA: Public Utilities Report, 1995) at 69-92.

249 16 Tex. Admin. Code § 25.243(e)(1).

250 16 Tex. Admin. Code § 25.243(e)(4).

modernization rider evaluated the financial health of First Energy's Ohio utilities and how the rider would be used to grid modernization.[251] The Commission found that the rider "would provide a needed incentive to the Companies to focus innovation and resources on grid modernization."[252] The Commission also found that the rider was "necessary to assist the Companies in accessing the capital markets in order to make needed investments in their distribution systems."[253, 254]

Pennsylvania has a statutory requirement for the evidentiary burden borne by the utility petitioning for approval of a distribution system improvement charge. Under state law, a utility must provide supporting evidence including:

> 2) *Testimony, affidavits, exhibits or other evidence that demonstrates that a distribution improvement system charge is in the public interest and will facilitate utility compliance with the following:*
>
> a) *The provision and maintenance of adequate, efficient, safe, reliable and reasonable service consistent with section 1501 (relating to character of service and facilities).*
>
> b) *Commission regulations and orders relating to the provision and maintenance of adequate, efficient, safe, reliable and reasonable service.*
>
> c) *Any other requirement under Federal or State law relating to the provision and maintenance of adequate, efficient, safe, reliable and reasonable service.*[255]

The question of need is complicated but answering it will clarify the conditions under which an alternative rate mechanism can be deployed and what types of costs can be recovered.

QUESTION #3:
HOW TO DESIGN THE ALTERNATIVE RATE MECHANISM TO PROTECT THE PUBLIC INTEREST?

Alternative rate mechanisms can shift the risk allocation between ratepayers and the utility. Utility commissions and state legislatures have a variety of procedural and substantive design tools at their disposal to ensure that use of the alternative rate mechanism is in the public interest. The following is a discussion of the design tools and how they have been and can be employed to protect the public interest while facilitating directed investment in areas of need.

251 Public Utilities Commission of Ohio, Case No. 14-1297-EL-SSO, Fifth Entry on Rehearing, October 12, 2016 at 87-89.
252 *Id.* at 87.
253 *Id.* at 90.
254 Please note that the use of this rider was invalidated by the Supreme Court of Ohio on the grounds that the distribution modernization rider did not qualify as an incentive under the Electric Security Plan statute and the conditions placed on the rider did not adequately protect ratepayers. IN RE Application of OHIO EDISON COMPANY, Cleveland Electric Illuminating Company, and Toledo Edison Company for Authority to Provide for a Standard Service Offer Pursuant to R.C. 4928.143 in the Form of an Electric Security Plan 157 Ohio St.3d 73 Supreme Court of Ohio, June 19, 2019.
255 66 Pa. Const. Stat. § 1353(b)(2).

Restricted Purpose

Many states condition the use of alternative rate mechanisms on achieving either a general public benefit or a specified result. By constricting the potential uses of the alternative rate mechanism, the number of opportunities to use the mechanism is naturally narrowed and the instances of use are all related. This selection protocol can reduce the burden on stakeholders participating in the process and the utility commission leading the approval and review processes.

The most common way to restrict the availability of the cost recovery mechanism is to limit it to the recovery of the distribution system investments. Additionality is often a core component of these statutes, seeking investment in new resources and not allowing the transfer of already planned and approved investments out of the regular cost recovery process. In Virginia, eligible projects must fall into one of the designated categories contained within the definition of an "electric distribution grid transformation project."[256] In Minnesota, to be an eligible distribution system investment, the project must be certified as a priority project.[257] Every two years, the Minnesota Public Utilities Commission certifies or denies proposed eligible distribution system projects.[258] A Minnesota utility is responsible for identifying investments that it believes necessary to "modernize the transmission and distribution system by enhancing reliability, improving security against cyber and physical threats, and by increasing energy conservation opportunities ..."[259] The Commission then evaluates the proposed investments to determine if the project deserves priority status. Importantly, the Commission has the authority to determine what is necessary to certify a project and can craft its own interpretation of the statute on a case-by-case basis.[260]

A note of caution, the authorizing statute should not be overly narrow. For example, Kansas has a gas system reliability surcharge (GSRS) that is used to incentivize and focus investment in the state regulated natural gas distribution system.[261] The statute was recently amended to permit use of the GSRS for the recovery of investments in the system and not solely for replacement of existing components.[262] Prior to the amendment, the language of the statute only allowed the GSRS to be used for eligible infrastructure system replacements.[263] It is expected that the change will allow investments in other priority areas like cybersecurity, safety plans, and replacement of obsolete legacy equipment.[264]

When state statutes are broadly framed, utility commissions have the authority to determine what is in the public interest and to provide the necessary restriction to focus the alternative rate mechanism so that it maximizes the benefit produced for the public.

256 Va. Code Ann. § 56-576.
257 Minn. Stat. § 216B.16(7b)(i).
258 Minn. Stat. § 216B.2425(1).
259 Minn. Stat. § 216B.2425(2)(2)(e).
260 Minnesota Public Utilities Commission, Docket No. E-002/M-15-962, Order Certifying Advanced Distribution-Management System (ADMS) Project Under Minn. Stat. § 216B.2425 and Requiring Distribution Study at 9.
261 Kan. Stat. Ann. § 66-2202-2204.
262 Kan. S.B. 279 (2017).
263 *Id.*
264 Leo Haynes, Kansas Corporation Commission, Neutral Testimony on Senate Bill 279, Submitted to House Energy, Utilities, and Telecommunications Committee, March 14, 2018 at 3.

For example, the Ohio law authorizing the use of various alternative rate mechanisms also directs the Commission to:

> *examine the reliability of the electric distribution utility's distribution system and ensure that customers' and the electric distribution utility's expectations are aligned and that the electric distribution utility is placing sufficient emphasis on and dedicating sufficient resources to the reliability of its distribution system.*[265]

In applying the law, the Public Utility Commission of Ohio framed the purpose of a distribution investment rider as facilitating "the timely and efficient replacement of aging infrastructure to improve service reliability."[266] By using this framing, the Commission focuses the utility's immediate efforts and provides a future platform for assessing the success of the utility's program.

Conversely, utility commissions can and should deny applications for alternative rate mechanisms when they will not produce a benefit for the public. The Maryland Public Service Commission denied access to an alternative rate mechanism because the proposed investment did not match the intended purpose for which the rate mechanism was implemented. In 2013, Pepco petitioned for and received approval for a Grid Resiliency Surcharge that would enable it to accelerate infrastructure investments to increase the reliability and resiliency of its distribution system.[267] The Commission approved the cost recovery mechanism on the grounds that it accelerated needed reliability work and would exceed the scope of the utility's plan to realize its annual performance standards.[268] When Pepco sought to renew the cost recovery mechanism, the Commission denied the application on the grounds that none of the proposed work was needed to meet the reliability standards established by regulation.[269]

Financial Triggers and Rate Caps

The financial consequences of permitting recovery outside of a general rate case are a major source of the pushback against the use of alternative rate mechanisms. The financial consequences must be weighed for the utility and for the ratepayer. An alternative rate mechanism should only be used to recover investment or operations and maintenance costs that would otherwise have a significant, demonstrable impact on the financial condition of the utility that would limit the utility's ability to invest if recovery was delayed. Moving significant amounts of cost recovery outside of a general rate case proceeding reduces the due process and the degree of oversight given to investment decisions which can negatively impact ratepayers. To find a middle ground where the financial consequences are significant for utilities and not excessive for ratepayers,

265 Ohio Rev. Code Ann. § 4928.143(B)(2)(h).

266 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.

267 Maryland Public Service Commission, Case No. 9311, Order 85724, In the Matter of the Application of Potomac Electric Power Company for an Increase in its Retail Rates for the Distribution of Electric Energy, July 12, 2013.

268 *Id.* at 160.

269 *Id.* at 75.

legislatures and commissions often use minimum and maximum investment levels to bound how much cost recovery can occur outside of a general rate case proceeding.

Minimum investment levels can ensure that the level of investment has risen to a point where there is a financial impact on the utility. Minimum investment levels can be a fixed-dollar amount, or a percentage of the revenue requirement. For example, under Illinois law, the large IOUs were allowed to recover costs for distribution grid modernization projects via a performance-based formula rate tariff provided that they put forth plans to invest at least $1.3 billion over a ten-year period, which included investments in smart grid technology and cybersecurity.[270] In Kansas, a natural gas utility may not file for the surcharge if the proposed amount to be recovered is the lesser of 0.5% of the base revenue requirement from the last general rate proceeding or $1,000,000.[271]

Maximum investment limits constrain potential impacts on ratepayers for investment costs recovered outside of a general rate case proceeding. When paired with minimum investment requirements, maximum investment limits help balance the tension between public interests and utility interests by capping the total amount of funds that can be recovered outside of a general rate case. The rate caps, like those for minimum investment levels, can either be a fixed-dollar amount or a percentage of revenue received. For example, in Ohio, the Commission modified the revenue caps for how much could be recovered each year from the Distribution Investment Rider authorized in AEP Ohio's Electricity Security Plan.[272] While under Pennsylvania law, recovery from the Distribution System Investment Charge is capped at 5% of distribution rates billed.[273] Similarly, in Kansas, revenue collected from the surcharge cannot exceed 20% of the base revenue requirement from the last general rate case proceeding.[274]

Return on Investment Constraints

Controlling the rate of return on investment is another tool at the disposal of commissions. Mandating a specific return on investment can control the impact on ratepayers. In Minnesota, the return on investment is set at the level approved in the utility's last general rate case, unless the commission determines that a different return is consistent with the public interest.[275] In Texas, the return on investment varies in accordance with when the last general rate case was completed. If a rate case was completed within the last three years, then the return on equity approved in the rate case is applied to the DCRF.[276] If more than three years have passed, a regulatory formula is used to calculate the return on investment.[277]

270 220 Ill. Comp. Stat. 5/16-108.5(b)(1)(B).
271 Kan. Stat. Ann. § 66-2303(a).
272 *Supra* note 263 at 18.
273 66 Pa. Const. Stat. § 1358(a)(1).
274 *Supra* note 271.
275 Minn. Stat. § 216B.16(7b)(6).
276 16 Tex. Admin. Code § 25.243(d)(2).
277 *Id.*

Filing Requirements

Filings requirements are a tool that can be deployed to protect ratepayer interests and generate information for commission review. Whether it is a procedural limitation or a substantive content requirement, placing conditions on utility access to the alternative rate mechanism is a simple way to produce ratepayer benefit and serve the public interest.

A common qualifier for utilities seeking approval for an alternative rate mechanism is that they have or will file a general rate case. Both Pennsylvania and Kansas have five-year qualification requirements. In Pennsylvania, the utility must certify that a base rate case has been filed within five years prior to the petition.[278] In Kansas, the Commission shall not approve a GSRS for any utility unless the utility has had a general rate case proceeding decided within the past 60 months or is engaged in an ongoing proceeding.[279]

In other jurisdictions, the number of opportunities to file for a rate adjustment are limited. By limiting the number of filings, commissions reduce rate volatility. Limiting the number of filings can improve workload management for the commission and the commission staff. Additionally, a smaller number of filings can reduce the cost of evaluating filings relative to the benefit provided. For example, Texas allows utilities to make one filing per calendar year and utilities may not change their rates more than four times between base-rate proceedings.[280]

Utilities can also be required to have a detailed investment plan approved before being granted access to an alternative rate recovery mechanism. This enables spending proposals to be pre-approved, but still subject to post-completion prudency reviews. This type of filing requirement also allows a commission to evaluate the entirety of a utility's investment program and to identify gaps and overlaps. It is also a natural place for inserting an option that utilities prepare some form of cybersecurity plan and provide it to the commission. In Pennsylvania, utilities must have filed a long-term infrastructure improvement plan before they are eligible to petition to use the Distribution System Improvement Charge.[281] In Minnesota, utilities must be operating under a multi-year plan and it must file a report on investments it considers necessary to modernize the transmission and distribution system.[282] In Ohio, approval of an electric security plan enables a utility to request cost recovery via an alternative rate mechanisms.[283]

Metrics

Access to an alternative rate mechanism can also be conditioned on the use of metrics to evaluate the effectiveness of the investment. For example, in Illinois, utilities seeking to recover grid modernization investment costs through a performance-based rate formula were required to file metrics with the Commission within 30 days of the approval of their tariff.[284] See Section 5 for information on the inclusion of metrics in grid modernization efforts.

278 66 Pa. Const. Stat. § 1353(b)(3).
279 Kan. Stat. Ann. § 66-2303(b).
280 16 Tex. Admin. Code §25.243(c)(1)(C).
281 *Supra* note 273.
282 Minn. Stat. § 216B.16(2)(e).
283 Ohio Rev. Code Ann. § 4928.143(F).
284 220 Ill. Comp. Stat. 5/16-108.5(c)(4)(A).

Prudency Reviews

Evaluating the prudency of revenue being recouped via an alternative rate mechanism is a common design feature. Mid-project and post-project reviews enable a utility commission to assess the status of a program or project and to perform. In Pennsylvania, a utility collecting revenue via the DISC is subject to audits at intervals determined by the Commission.[285] In Ohio, utilities operating under an electric security plan are subject to annual reviews to determine whether they have excessive earnings.[286]

More common is the review of revenues from the alternative rate mechanism in the next general rate case proceeding. For example, approval of use of an alternative rate mechanism can be conditioned on filing a general rate case. In Maryland, the Commission required a utility to file a base rate case that aligned with the projected completion date of the qualifying projects, and it ordered that the projects and the revenue were subject to a full prudency review.[287]

Sunset Clauses

Sunset or termination clauses are deployed to limit the lifespan of an alternative rate mechanism and its impact on rates. A legislature or commission may restrict access to the alternative rate mechanism for a specified time period to direct investment into specific areas of need. The termination clause can target the availability of a specific cost recovery mechanism or limit a utility's use of the mechanism. Pennsylvania requires that the Distribution System Investment Charge be reset to zero after the new base rates are established in a general rate case proceeding.[288] Kansas has a similar treatment for revenues collected through the GSRS.[289] In Ohio, AEP's distribution investment rider will expire at the end of 2020 unless the utility files a rate case by June 1, 2020.[290]

Conclusion

The concern about the impact of regulatory lag on cyber preparedness is a valid concern that warrants investigation. Cybersecurity investments have different characteristics than traditional utility investments. Their lifespans are shorter than traditional utility investments and carry a greater likelihood of redundancy. Those special characteristics create special challenges for incentivizing the investment that is needed to maintain and enhance protections levels.

As cybersecurity investment levels grow, the potential impact of regulatory lag will grow too. This section offered a series of steps and principles that can be used to determine whether regulatory lag is negatively impacting current and future cybersecurity investment levels. By assessing the impact of regulatory lag on utility investment within the context of the overall financial status of the utility, commissions can determine whether alternative rate mechanisms are needed. If it is determined that there is a need, the section laid out multiple options for designing and administering the alternative rate mechanism in a manner that serves the public interest.

285 66 Pa. Const. Stat. § 1358(e)(1).
286 Ohio Rev. Code Ann. § 4928.143(F).
287 *Supra* note 265 at 162.
288 66 Pa. Const. Stat. § 1358(b).
289 Kan. Stat. Ann. § 66-2204(f)(1).
290 *Supra* note 266 at 80.

SECTION 5
METRICS

METRICS ARE CRUCIAL TO THE SUCCESS of a utility's cybersecurity program. Cybersecurity threats are growing in number and sophistication.[291] To adapt to everchanging circumstances, utilities will need a cybersecurity program that is continuously improving. Continuous improvement comes through a rigorous program of self-assessment and evaluation. Metrics allow for utilities to self-assess their security posture by quantifying information into comparable values. Metrics also support decision-making by evaluating past performance and predicting results of future investment and policy changes.

Metrics provide a simple, consistent way to communicate system security to a range of stakeholders including utility commissions. As cybersecurity threats and investments grow, the value of cybersecurity metrics is magnified. Utilities need metrics to evaluate system security, and utility commissions need metrics to evaluate the effectiveness of utility investments and policy decisions. Increasing amounts of investment in grid modernization efforts and cybersecurity protections will increase questions about cost effectiveness and utility performance. Resiliency metrics are necessary to understand what areas of the grid need improvement and to justify investment in those areas.[292]

A gap exists between what resiliency metrics the utility sector needs and what tools are available. The electric utility sector lacks a common set of accepted resiliency metrics. Reliability metrics are not suitable for measuring resiliency and utility performance because reliability metrics focus on normal operating conditions while resiliency metrics

291 EPRI, Cybersecurity Roadmap (2018) at 8.
292 National Academy of Sciences, Enhancing the Resilience of the Nation's Electricity System (2017) at 31.

measure preparedness and response to low frequency, high consequence events.[293] In 2013, the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21) highlighted the absence of resiliency-specific metrics.[294] In 2017, a National Academy of Sciences report concluded that more research is needed before a consensus is reached on which metrics are essential.[295]

Multiple efforts addressing this gap are starting to bear fruit. The considerable resources invested into developing, refining, and piloting resiliency metrics at the Electrical Power Research Institute (EPRI), Sandia National Laboratory, Pacific Northwest National Laboratory, Grid Modernization Laboratory Consortium, and other public and private researchers are creating the foundation for a broad deployment of grid resiliency and cybersecurity metrics.[296] Dozens of utilities contribute to EPRI's cybersecurity metrics development program by allowing their data to be used to evaluate and refine metrics.[297] The Grid Modernization Laboratory Consortium is producing tools to allow operators to anticipate, respond to, and recover from extreme events.[298]

Development Considerations for Metrics

Standards-based metrics like NERC-CIP, ES-C2M2, and NIST-CSF are gaining a foothold in utility cybersecurity practices.[299] These standards offer value to utilities and utility commissions, but they have limitations. It is important to have standards, but it is more important not to stop with the development of standards, to go beyond standards into the deployment of metrics. As EPRI wrote:

> *Security standards/guidelines are not the same as security metrics. Security metrics should facilitate analysis and discussion, while providing insight into program improvements or gaps. Standards/guidelines provide a common taxonomy for discussing cyber security threats and vulnerabilities. Some standards detract the focus from process improvement towards compliance.*[300]

293 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.

294 The White House, 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.

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

296 EPRI's Cybersecurity Metrics program has been operating for the past half decade and has built out a considerable portfolio of current and future research papers, see EPRI, Creating Cyber Security Metrics for the Electricity Sector, Version 2.0 (2016) and EPRI, Creating Cyber Security Metrics, Volume 3 (2017). Sandia National Laboratories, Resilience Metrics for the Electric Power System: A Performance-Based Approach (2017); Grid Modernization Laboratory Consortium, Foundational Metrics Analysis https://gmlc.doe.gov/projects/1.1; H. Willis and K. Loa, RAND Corporation, Measuring The Resilience of Energy Distribution Systems (2015); Alexis Kwasinski, Quantitative Model and Metrics of Electrical Grids' Resilience Evaluated at a Power Distribution Level, Energies 9 (2016) https://pdfs.semanticscholar.org/b6cf/ec805511b20557c14233b739bd6c8198c990.pdf.

297 EPRI, Creating Cyber Security Metrics for the Electric Sector: Volume 3 (2017) at iii-iv.

298 Grid Modernization Laboratory Consortium, 1.5.01 Grid Resilience and Intelligence Platform (GRIP), https://gmlc.doe.gov/resources/1.5.01-grid-resilience-and-intelligence-platform-grip.

299 *Supra* note 1 at 52-54.

300 EPRI, Creating Cyber Security Metrics for the Electric Sector (2016) at 2-3.

The development of metrics often starts with the development of standards and guidelines that focus on compliance with a specific set of regulations or the provision of a specific set of assurances. The question is how to build upon the standards-based metrics to get to best practices focused metrics as it the best practices metrics that will provide the continuous improvement necessary to meet the cybersecurity challenge.

The transition from standards-based metrics to best practices metrics will require a series of steps from selecting the metrics to refining the metrics. The metrics build out will be layered; building up capacity to record, monitor, and assess within utilities and building up the capacity to process, evaluate, and direct within utility commissions.

SELECTING METRICS

The selection of metrics should reflect what metrics are available, what metrics have been tested, and what utility resources are required to implement usage of the metric. Metrics should be considerate of utility processes and the grid architecture of legacy systems.[301] Metrics should have clear purposes: assisting in the evaluation of a utility's security posture and risk management programs and/or evaluating the effectiveness of individual investments and policy decisions. The metrics should create feedback loops that inform operational decisions and investment plans.[302] If desired, metrics can be a condition to the use of alternative rate mechanisms.

The process of selecting metrics must include security concerns. Metrics can be used to test a utility's defenses and to simulate a response to an incident. This information is valuable to the utility and to threat actors. Protecting this information is part and parcel in preserving the stability of a utility and measures must be taken to limit or prevent the dissemination of the information. In all circumstances, the vulnerability of reporting and recording the metrics should be weighed and appropriate measures taken to protect confidential information, see Section 2.

Lastly, it is important to note that the preferred set of metrics will change in accordance with technology and knowledge of risks and vulnerabilities. Both the metrics produced from a process and the process of identifying metrics should change as entities gain knowledge, sophistication, and familiarity. The metrics can transition from consistent use of attributed-based standards to more progressive performance-based analyses. Existing frameworks and standards like NERC CIP, NIST CSF, and ES-C2M2 can be used to establish initial baselines, and then built upon by more advanced metrics.

WINNOWING DOWN THE OPTIONS

There are a lot of possible metrics available, which is why the process of selection must be deliberate and comprehensive. Metrics can be attribute-based assessments of a utility security's system or performance-based evaluations of a utility's actual or simulated response to an incident. Metrics can identify gaps in defense and evaluate best available, cost-effective solutions. They can look at technological and policy solutions. Resiliency

301 Pacific Northwest National Laboratory, Electric Grid Resilience and Reliability for Grid Architecture (2017) at 2.

302 Grid Modernization Laboratory Consortium, Grid Modernization: Metrics Analysis (GMCL 1.1) Reference Document, Version 2.1 (2017) at 4.24.

metrics can look at cyber threats or cyber threats plus natural threats to grid stability. They can be combined to create a holistic view of a utility's cybersecurity posture. Metrics can cover information technology and operational technology security; utility governance; intra- and inter-utility communication protocols; and all aspects of resiliency (robustness, resourcefulness, recovery, and adaptation).[303]

Metrics development and selection should take advantage of existing resources and capacity while building out capacity to add more sophisticated analyses. Metric selection and maturity are processes of identification and refinement; thus, the preferred set of metrics will change in accordance with technology and knowledge of risks and vulnerabilities.

A Pathway for Incorporating Resiliency Metrics

The work on the technical aspects of quantifying resiliency should be paired with an expanded inclusion of resiliency metrics in utility commission proceedings and dockets. Commissions should work to define resiliency objectives and goals and explore how metrics can assist them in achieving measurable results. The process can start with a discussion of how resiliency metrics can become a consistent part of utility performance evaluations and investment proposals. Commissions have the power to institute metrics for individual utilities and for state-wide comparisons. The combination of actions could advance the formation of industry-accepted metrics for aggregated benchmarking and individual utility performance.

Metrics do not spontaneously emerge, they gain acceptance by research, development, deployment, and refinement. Reliability frequency indices Customer Average Interruption Frequency Index (CAIFI) and System Average Interruption Frequency Index (SAIFI) and reliability duration indices Customer Average Interruption Duration Index (CAIDI) and System Average Interruption Duration Index (SAIDI) are now widely accepted and widely adopted. The acceptance and use of these indices a result of two decades of research and deployment.[304] The standards were first issued by the IEEE Standards Association in 1999. The advancement of the metrics also created a pathway for feedback that can guide the refinement process. Since 1999, the IEEE has issued two revisions, with a third in the planning stages, of its distribution reliability indices and factors.[305]

State Examples

There is an absence of examples of utility commission development of resiliency metrics that commissions can draw upon for guidance. Fortunately, there are a multitude of examples of how utility commission have developed and deployed reliability metrics and grid modernization project-specific metrics to demonstrate possible pathways for building

303 NERC Reliability Issues Steering Committee, Report on Resiliency, November 8, 2018 at 5.

304 IEEE Standards Association, P1366 – Guide for Electric Power Distribution Reliability Indices, 2018 https://standards.ieee.org/project/1366.html; IEEE Standards Association, IEEE 1366-2012 - IEEE Guide for Electric Power Distribution Reliability Indices, 2012 https://standards.ieee.org/standard/1366-2012.html; IEEE Standards Association, IEEE 1366-2003 - IEEE Guide for Electric Power Distribution Reliability Indices, 2003 https://standards.ieee.org/standard/1366-2003.html; IEEE Standards Association, IEEE 1366-1998 - IEEE Guide for Electric Power Distribution Reliability Indices, 1998 https://standards.ieee.org/standard/1366-1998.html.

305 *Id.*

resiliency and cybersecurity metrics into utility commission practices. The examples emphasize the value of consultation with stakeholders and experts and the need to devote resources to the process. They also show how standards should evolve and how the development process should be open-ended to align metrics with best available data and knowledge. Lastly, the examples show how legislatures can initiate a metrics development process, but the best location for the promulgation and evaluation of the metrics is the utility commission.

CALIFORNIA

California provides an example of how to address the complicated issues that can arise from the development of cybersecurity metrics. Concerns about privacy of confidential information, risks to system security, and metric functionality may not receive adequate attention in the course of a proceeding that is addressing multiple items. Finding an alternative platform, like a technical working group, is an option that allows for consultation from a wide swath of stakeholders on a focused set of issues.

In 2012, the California Public Utilities Commission issued an order adopting metrics for the smart grid deployments of PG&E, SCE, and SDG&E.[306] The decision established metrics for the deployment of smart grid technology and it created a technical working group for the purpose of establishing cybersecurity goals metrics.[307] The Commission found that physical security and cybersecurity are key components of the smart grid, but it declined to order a set of metrics be included in smart grid reporting.[308] The Commission wrote "[w]e conclude that the limited record developed in this point is insufficient to adopt a full set of useful and informative metrics that are not unduly burdensome."[309]

Two years later, in a docket focused on metrics, the Commission acknowledged that there was no consensus on what cybersecurity metrics should be used by utilities and set forth a plan to use a technical working group to work on the substance and process of cybersecurity metrics. A similar plan was employed for environmental metrics as neither cybersecurity nor environmental metrics was "subject to the straightforward quantification that would permit the construction of a simple metric" despite both being of "critical policy significance."[310]

The Commission's discussion and decision provides insight into how a technical working group might be structured and directed. Stakeholder comments focused on the security of the technical group meeting and how to deploy non-disclosure agreements and other security practices to facilitate discussion without increasing risk.[311] The Commission, in response, wrote that "utilities will not be required to disclose cyber-security gaps and vulnerabilities, cryptographic and software protective measures, or other similar items in the workshop."[312] The Commission furnished a non-exhaustive list of questions,

306 California Public Utilities Commission, Decision 12-04-025, Decision Adopting Metrics to Measure Smart Grid Deployments of Pacific Gas and Electric Company, Southern California Edison Company and San Diego Gas & Electric Company, April 19, 2012.
307 *Id.* at 52.
308 California Public Utilities Commission, Decision 10-06-047, Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, June 24, 2010 at 58, 84.
309 *Id.* at 84.
310 *Supra* note 306 at 30.
311 *Supra* note 306 at 30-32.
312 *Supra* note 306 at 35.

albeit attribute-focused, to serve as a starting point for discussion in the working group.[313] Additionally, the Commission recommended that the forum serve as the place for discussing what policies were needed to address cybersecurity issues with legacy equipment.[314] Furthermore, in the 2010 decision, the Commission required that each utility include grid security and cybersecurity in their annual Smart Grid reports along with the consensus metrics.[315]

MARYLAND

Maryland's experience with reliability metrics provides an example of how a legislature and commission can split duties in the development of metrics. A legislature can initiate action on adopting metrics, but it is the commission that is best equipped to oversee the process. Regular reviews of the efficacy of the metrics and the ability to impose different goals on utilities based upon their unique characteristics are important components of creating a metrics program capable of driving improved performance.

In 2011, Maryland passed the Electric Service Quality and Reliability Act designating reliability standards that utilities must meet and directing the Public Service Commission to develop regulations necessary to implement the program. The legislation contains multiple elements that could be used to develop a utility reporting requirement for system resiliency including tailoring the requirements, using Commission expertise, and continually revising the performance goals.

Maryland tailored the metrics program to match the institutional capacity of its utilities. The legislation had a restricted applicability, only applying to utilities with more than 40,000 customers, thus exempting small rural electric cooperatives and municipal electric companies.[316] The reporting requirements differ for investor-owned utilities and electric cooperatives, with the latter exempted from being subject to the corrective action and civil penalty provisions.[317]

The Legislature selected most of the performance metrics while giving authority to the Commission to implement and evaluate the standards. The statute states that the utilities will annually report their SAIFI and SAIDI performance results and "any other performance measure that the Commission determines to be reasonable."[318] Additionally, the law prescribed a list of elements that the regulations shall include, which included service interruptions, downed wire response, periodic equipment inspections, and any other standards established by the Commission.[319] However, the law designated the Commission as the responsibility party for overseeing the development of the regulations adopting the standards,[320] updating the standards,[321] receiving the annual performance reports,[322] and

313 *Supra* note 306 at Attachment B.
314 *Supra* note 306 at 35.
315 *Supra* note 308 at 84-85.
316 Md. Code Ann. § 7-213(c)(1).
317 Md. Code Ann.§ 7-213(f)(2)(i).
318 Md. Code Ann. § 7-213(d)(1-3).
319 Md. Code Ann. § 7-213(e)(1)(i).
320 Md. Code Ann. § 7-213(d)(1).
321 *Id.*
322 Md. Code Ann. § 7-213(g)(1).

certifying compliance with the standards.[323] Lastly, the law allowed for the creation of a separate reliability standard for each utility to account for system reliability differentiating factors, including system design and existing infrastructure.[324]

The Commission developed regulations to establish SAIDI and SAIFI standards for four-year cycles. In 2011, the Commission opened a rulemaking proceeding to establish the SAIDI and SAIFI reliability standards for the years 2012-2015.[325] In 2015, using the same docket, the Commission established the standards for 2016 through 2019. The standards require utility performance to incrementally improve over each calendar year.[326] The standards are finalized after stakeholders are given the opportunity to comment on the staff proposal.

MASSACHUSETTS

Massachusetts is an example of how resiliency and cybersecurity metrics could be developed from a new commission docket or could evolve out of an existing utility reporting requirement. The Massachusetts case study provides several important points. First, metrics development is a continuous process. Metrics can and should evolve to reflect best available knowledge and it is acceptable to remove metrics that no longer provide value (e.g. assess or direct company performance, investments, and policy decisions). The process of developing metrics should take a broad initial stance on what metrics to include, being proactive and future-forward allows for more open discussions. Moreover, what is excluded now may be added during a later proceeding. Metrics are restricted by what information is available to establish baselines, so focus on collecting information to feed into the process. Lastly, metrics should start by concentrating on recording and reporting utility performance before moving to incentivizing and penalizing utility performance.

Massachusetts Grid Modernization Efforts

Massachusetts, like many other states, initiated grid modernization proceedings in the past decade. In 2012, the Massachusetts Department of Public Utilities filed a Notice of Investigation into the modernization of the electric grid with the purpose of investigating policies that would enable electric distribution companies and their customers to take advantage of grid modernization opportunities.[327] Massachusetts prioritized the development of utility-specific metrics and statewide metrics to assess the achievement of grid modernization objectives and the performance of grid modernization investments.

In 2014, the Department issued its grid modernization order requiring that each electric distribution company submit a ten-year grid modernization proposal and that each utility

323 Md. Code Ann. § 7-213(f)(1).
324 Md. Code Ann. § 7-213(e)(2).
325 Maryland Public Service Commission, RM 43 Revisions to COMAR 20.50 Service Supplied by Electric Companies - Proposed Reliability and Service Quality Standards, Notice of Initiating Rule Making, Notice of Comment Period, and Notice of Rulemaking Session, January 12, 2011.
326 Md. Code Regs. 20.50.12.02(D)(1).
327 MA DPU 12-76 Massachusetts Electric Grid Modernization Stakeholder Working Group Process: Report to the Department of Public Utilities from the Steering Committee, (2013) at 2.

propose metrics tied to its grid modernization goals.[328] Each electric distribution company was directed to propose "two types of company-specific metrics: (1) infrastructure metrics that track the implementation of grid modernization technologies and systems; and (2) performance metrics that measure progress towards the objectives of grid modernization."[329] Additionally, the companies were directed to jointly propose a common list of statewide metrics.[330] To assist the utilities, the Department provided an illustrative, but non-exhaustive list of potential metrics based on the identified grid modernization objectives: reducing the effects of outages; optimizing demand, including reducing system and customer costs; integrating distributed resources; and improving workforce and asset management.[331]

Each company was required to include in its grid modernization plan, a description of the process used to develop the company-specific and statewide metrics, the definitions and formulas used, and how the metric connects to the grid modernization objective.[332] Importantly, the order set out that companies should include metrics that "measure outcomes that may not be within the companies' complete control" and to develop metrics for grid modernization goals that are not easily quantified, in order to capture those benefits.[333] The companies were required solicit stakeholder input in the development of the metrics and to provide a summary of the solicitation process in their grid modernization plan submission.[334] Lastly, the Department decided that the purpose of the metrics would be, for now, to record and report information, and that the metrics would not be tied to incentives or penalties.[335]

National Grid, Eversource, and Unitil submitted their grid modernization plans in August 2015, which included suggested company-specific and statewide metrics.[336] In May 2018, the Department issued its decision on the plans and provided additional direction on the development of the metrics.[337] The three companies had submitted a variety and range of metrics for approval. National Grid submitted seven statewide and eight company-specific metrics and approved National Grid's modernization plan.[338] Unitil submitted sixteen metrics.[339] Eversource submitted two statewide metrics and one company-specific metric for customer-facing investments and fourteen metrics for grid-facing investments.[340]

The Department sought to simplify and clarify what metrics would be deployed to assess

328 Massachusetts Department of Public Utilities, D.P.U. 12-76-B, Investigation by the Department of Public Utilities on its own Motion into Modernization of Electric Grid, June 12, 2014 at 30.
329 *Id.* at 30.
330 *Id.* at 30.
331 *Id.* at 31-32.
332 *Id.* at 32-33.
333 *Id.* at 33.
334 *Id.* at 33-34.
335 *Id.* at 34.
336 Massachusetts Department of Public Utilities 15-120; Massachusetts Department of Public Utilities 15-122; Massachusetts Department of Public Utilities 15-121.
337 Massachusetts Department of Public Utilities, MA DPU 15-120; MA DPU 15-122; MA DPU 15-121, Petitions for Approval of Grid Modernization Plans, May 10, 2018.
338 *Id.* at 188.
339 *Id.* at 189.
340 *Id.* at 189-190.

grid modernization achievements and performance. The Department found that it was necessary to streamline the information provided to the Department and stakeholders and thus prescribed the use of the same company-specific metrics for tracking a utility's deployment of grid-facing investments.[341] The Department declined to approve specific grid-facing performance metrics based on the need for additional work to connect with metrics with the asserted benefits.[342] Instead, the utilities were ordered to revise their metrics and participate in a Department-convened stakeholder process to review the metrics.[343] The revised metrics were submitted in June 2019.[344]

Service Quality Standards

Massachusetts' service quality and reliability reporting standards provide another example of how metrics should evolve to fit system assessment needs and how metrics should change as new sources of data become available. Under Massachusetts law, gas and electric utilities must submit reports that detailing their performance in meeting the Department-approved service quality guidelines.[345]

The service quality guidelines emerged from a 1999 law allowing for performance-based rate schemes for distribution, transmission, and gas companies.[346] To implement the law, the Department issued a Notice of Inquiry (NOI) shortly thereafter.[347] The NOI outlined a proceeding that would determine service quality plan and the penalty mechanism. The proceeding would examine the types of performance measures that should be included in the plan, the manner by which performance would be measured, and the method by which benchmarks for employee staffing levels and training programs would be established.[348]

In the order establishing the performance benchmarks, the Department was open to data from the companies and from outside the state. The Department stated service quality performance benchmarks would be established using the historical performance of the companies. But, the Department required the companies to collect data that could enable the Department, in the future, to evaluate company performance against national or other regional performance measures.[349] The Department directed each company to submit a written report detailing individual collection efforts, identifying what nationwide, regionwide, and statewide performance data is potentially available for a comprehensive database, and assessing the feasibility of establishing a cooperative approach to comparative benchmarking.[350] Reliability metrics, that enjoy common usage today, were assessed and evaluated for inclusion in the performance benchmarks, including CAIDI,

341 *Id.* at 200-201.
342 *Id.* at 202.
343 *Id.* at 202.
344 Massachusetts Department of Public Utilities, MA DPU 15-120; MA DPU 15-122; MA DPU 15-121, Grid Modernization Plan Performance Metrics, Revised June 6, 2019.
345 Mass. Gen. Laws ch. 164 § 1E.
346 *Id.*
347 Massachusetts Department of Public Utilities, D.T.E. 99-84, Investigation by the Department of Telecommunications and Energy on its own Motion to Establish Guidelines for Service Quality Standards for Electric Distribution Companies and Local Gas Distribution Companies pursuant to G.L. c. 164, § 1E, October 29, 1999.
348 *Id.* at 2.
349 *Id.* at 4.
350 Id at 4.

SAIFI, and SAIDI.[351] Interestingly, CAIFI was not used because it did not provide the same opportunity for cross-company comparison as CAIDI.[352]

The service quality guidelines have continued to be updated since their initial promulgation. In 2006, the Department promulgated revised service quality guidelines and made changes to several measures and topics such as SAIDI and SAIFI.[353] It modified the exclusion criteria for SAIDI and SAIFI to require the inclusion of outages on non-primary/secondary circuits in the calculations.[354] They also amended the original standards to ensure that the quality of customer service did not deteriorate with performance-based rates.[355]

As of 2016 and moving forward, service quality standards shifted from preventing performance deterioration to requiring improved service quality.[356] In opening the investigation, the Department took a broad approach to what metrics might be considered. Comments were invited on the existing metrics and potential new metrics for safety and customer satisfaction, potential clean energy metrics, options for benchmarking metrics, and whether to add or delete any metrics.[357] The final order did not take the same broad approach, instead focusing on finetuning existing metrics and removing non-essential metrics. Benchmarks were also established that required improved performance over time, which departed from the prior practice of using fixed benchmarks.[358]

Conclusion

If commissions are going to move to a best practices-focused cybersecurity regime, resiliency metrics will be an essential component of their efforts. Research into resiliency metrics is identifying data points, testing metrics, and preparing them for deployment. Commissions should start the process of figuring out how to integrate resiliency metrics into utility reporting practices. Fortunately, the rise in use and acceptance of reliability metrics provides a roadmap for how commissions might introduce and popularize resilience metrics.

It will require time and resources to refine the metrics to maximize their value, but the investment will return benefits in excess of the costs. The process for selecting metrics should never cease. Once the metrics are established, commissions and utilities should evaluate the effectiveness of the metrics program, identify gaps where new metrics are needed, and discard unproductive metrics. By matching the refinement of the metrics with the refinement of the metrics selection process, utility commissions can foster an ethos of continuous improvement.

351 *Id.* at 12-13.
352 *Id.* at 12.
353 Massachusetts Department of Public Utilities, DTE 04-116-C, Investigation by the Department of Telecommunications and Energy on its own motion regarding the service quality guidelines established in Service Quality Standards for Electric Distribution Companies and Local Gas Distribution Companies, D.T.E. 99-84 (2001), April 10, 2007.
354 *Id.* at 2.
355 Massachusetts Service Quality Standards, www.mass.gov/service-details/service-quality.
356 *Id.*
357 Massachusetts Department of Public Utilities, D.P.U. 12-120, Investigation by the Department of Public Utilities on its own motion regarding the service quality guidelines established in Service Quality Standards for Electric Distribution Companies and Local Gas Distribution Companies, D.T.E. 99-84 (2001) and amended in Service Quality Standards for Electric Distribution Companies and Local Gas Distribution Companies, D.T.E. 04-116 (2007), December 11, 2012 at 2-3.
358 Massachusetts Department of Public Utilities, DPU 12-120-D, Order Adopting Revised Service Quality Guidelines, Dec.18, 2015 at 3.

SECTION 6

GRID MODERNIZATION AND CYBERSECURITY

THE GRID IS CHANGING AND CHANGING RAPIDLY. With the change comes an increased riskof a cyberattack and an opportunity to reorient utility commission practices to proactively tackle distribution utility cybersecurity posture. Millions of devices are connecting to the grid to bring renewable energy into the distribution system, to facilitate bi-directional flow of energy, and to enhance communication systems. Those connections increase the attack surface of the grid. Utility commissions across the country have opened or are opening grid modernization dockets to address issues arising from the rapid pace of change occurring on distribution systems. This section tackles how utility commissions can proactively control and shape the grid modernization process to get ahead of emerging issues.

The high level of grid modernization activity makes it an ideal candidate for addressing cybersecurity protections.[359] In just the second quarter of 2019, 33 states made 116 legislative or regulatory actions addressing grid modernization polices, 32 states and territories took 75 legislative or regulatory actions addressing grid modernization deployment, and 31 states and territories took legislative or regulatory actions addressing

359 For the purposes of this report, the definition of a grid modernization effort is that promulgated in the North Carolina Clean Energy Technology Center's 50 States of Grid Modernization quarterly reports. A grid modernization legislative or regulatory action includes (1) smart grid and advanced metering infrastructure, (2) utility business model reform, (3) regulatory reform, (4) utility rate reform, (5) energy storage, (6) microgrids, and (7) demand response. The number of grid modernization legislative and regulatory actions captured by this definition will be larger than the number of actions capable of addressing utility cybersecurity practices, but nonetheless the sheer volume of actions is demonstrative of the level of attention this area if receiving and thus its potential to affect cybersecurity reporting obligations. *Supra* note 220.

grid modernization studies or investigations.[360] There were more than 20 smart grid legislative and regulatory actions and more than 15 grid modernization legislative and regulatory actions ongoing during the second quarter alone.[361]

The Modern Grid

The pace of change on the grid creates an urgency to secure the grid. Eight states have set 100% renewable or clean energy goals.[362] By 2023, U.S. distributed energy resources[363] are predicted to more than double from 2017 levels from 46 GW to 104 GW;[364] going from millions of devices to hundreds of millions of devices. Rooftop solar installations in the United States topped 2 million in 2019 and are expected to double again by 2023.[365] By 2017, almost half of all meters installed in the United States were smart meters, a total of more than 70 million meters.[366] The cybersecurity implications of these coming changes are significant and early action will reduce vulnerabilities and risk.

The Grid Modernization Docket

Active grid modernization dockets[367] can be found across the United States. State legislatures, governors, executive agencies, utility regulators, and electric utilities are planning what their distribution grids will look like in the future. Multiple state legislatures and executive agencies are crafting laws and policies to guide and structure efforts to prepare for the grid of the 21st century. The pace of dockets being opened, and legislation being proposed follows the transformation of the grid. These developing laws and policies are an incredible opportunity to build cybersecurity into the norms of grid modernization.

The public utility commissions are and should be the primary organization overseeing a utility's grid modernization plan. Governor's offices and legislatures may play a key role in initiating grid modernization dockets and determining the parameters of a utility's grid modernization program, but it is the commission that plays the essential role of aggregating stakeholder input, defining the scope of the docket, and developing the processes that encourage participation and information sharing.

360 *Supra* note 221 at 6.

361 *Supra* note 221 at 10.

362 Jeff Deyette, Union of Concerned Scientists, States March Toward 100% Clean Energy – Who's Next?, August 28, 2019, https://www.ecowatch.com/clean-energy-united-states-2640084281.html?rebelltitem=1#rebelltitem1.

363 A distributed energy resource may be either physical or virtual. Distributed energy resources consist of a wide range of technologies including energy generation technology, energy storage technology, and grid operation technology.

364 Green Tech Media, "Distributed Energy Poised for 'Explosive Growth' on the US Grid," June 21, 2018 https://www.greentechmedia.com/articles/read/distributed-energy-poised-for-explosive-growth-on-the-us-grid#gs.484q5a.

365 Solar Energy Industries Association, United States Surpasses 2 Million Solar Installations, May 9, 2019, https://www.seia.org/news/united-states-surpasses-2-million-solar-installations.

366 Federal Energy Regulation Commission, 2018 Assessment of Demand Response and Advanced Metering – Staff Report, November 2018, https://www.ferc.gov/legal/staff-reports/2018/DR-AM-Report2018.pdf at 1.

367 For the purposes of this report, we adopt the definition of grid modernization developed by the North Carolina Clean Energy Technology Center which includes the following types of actions: (1) smart grid and advanced metering infrastructure, (2) utility business model reform, (3) regulatory reform, (4) utility rate reform, (5) energy storage, (6) microgrids, and (7) demand response. Autumn Proudlove et al., North Carolina Clean Energy Technology Center, 50 States of Grid Modernization, Q2 Quarterly Report – Executive Summary, July 2019, https://nccleantech.ncsu.edu/wp-content/uploads/2019/07/Q22019_gridmod_exec_final.pdf at 3.

The architecture and shape of the future grid will vary from state to state, but there are consistent elements that need to be included to ensure that cybersecurity is integrated into grid modernization efforts. Our research surveyed multiple grid modernization efforts and identified key elements that ensure that cybersecurity is included in a comprehensive manner and that processes are developed that encourage the identification and adoption of best practices. The elements are:

1. Defining cybersecurity
2. Defining scope of docket
3. Building processes that facilitate best practices

ELEMENT ONE: DEFINING CYBERSECURITY

A specific, unambiguous definition of cybersecurity eliminates uncertainty over what areas should receive attention in grid modernization planning processes, rate filings, and other proceedings. Legislators, regulators, and stakeholders should define cybersecurity as inclusive of information technology and operational technology and covering physical and virtual assets. Please see Section 2 for more detail on this topic.

Early cybersecurity protections focused on data privacy. Today, data privacy concerns must be managed alongside operational security of the grid. In fact, surveys of utility professionals indicate that there is greater concern about threats to the operational technology than to information technology.[368] Ensuring a balance of attention is allotted to data privacy and to grid operations will guide regulators and utilities towards a comprehensive view of the threats to utility systems. The source of that balance is a strong, granular definition that captures the complex combination of physical and virtual assets, and of information and operational technology that require cybersecurity protection. The following examples highlight options for defining cybersecurity that can orient grid modernization proceedings. With a shared understanding of what cybersecurity is, all stakeholders can grasp and tackle the challenge of protecting the modern grid.

NEW HAMPSHIRE

The New Hampshire Public Utility Commission (NHPUC) published an exemplar definition of cybersecurity that includes cyber protection for both infrastructure and customer data. In the 2019 NHPUC "Staff Recommendation on Grid Modernization" cybersecurity was defined as:

> *The protection of computer systems from theft or damage to the hardware, software, data, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to deviation from secure procedures.*[369]

368 *Supra* note 212 at 13.

369 New Hampshire Public Utilities Commission, IR 15-296 Investigation in Grid Modernization, Staff Recommendations on Grid Modernization, January 31, 2019 at 109.

VIRGINIA

Even when a comprehensive definition of cybersecurity is not provided by state law or in a commission order, utilities can respond with plans that allocate resources to information and operational technology. In 2018, Virginia enacted the Grid Transformation and Security Act, which defined an electric distribution grid transformation project as a project associated with electric distribution infrastructure that is designed, amongst other possible factors, to enhance cybersecurity.[370] Cybersecurity was not defined in the Act. Nonetheless, Dominion Energy submitted its plan and detailed its intention to:

> *continue to implement strict cyber security standards for all intelligent devices and automated control systems installed, replaced or upgraded under the Plan. All systems that collect information from customers, including data from smart meters or other information obtained through the new CIP, will have strong cyber security components. Information from these intelligent devices and systems will be comprehensively reviewed to detect and prevent any possible cyber intrusions that could threaten the Company and its customers.*[371]

By covering information and operational technology, Dominion established a baseline for protecting critical systems that could evaluated by the State Corporation Commission.

ELEMENT TWO: DEFINING SCOPE OF DOCKET – THIRD PARTY VENDORS

Attention to the impact of third-party vendors and suppliers on cybersecurity is an element that must be built into every grid modernization effort. Commissions have the greatest ability and opportunity to include this issue in dockets as they determine the scope of issues that utilities must address in their filings.

Grid modernization is changing the way that the grid operates and changing who is offering services on the grid. Third-party vendors and suppliers are providing a greater share of grid services as grid operations are digitized. Services that were once offered by a utility are now provided by a third party via the cloud. These third parties can come in the form of contractors or vendors working directly with the electric company, to outside DER developers that maintain active communication with technology connected with the grid. Rigorous external regulation and internal monitoring and investment can help keep utility's defenses up to date, but less oversight over third parties can affect the ability to implement and maintain safe cyber defenses. Whether it is a third-party owned DER or a third-party service provider, their connection with the grid alters the attack surface of the system and the security posture of the system. Thus, the inclusion and consideration of their impacts on system vulnerabilities is a critical element in any grid modernization proceeding.

A recent filing by AEP captures the changing nature of grid operation and the concern

370 *Supra* note 256.

371 Virginia State Corporation Commission, Case No. PUR-2018-00100, Dominion Application, Petition of Virginia Electric and Power Company, For approval of a plan for electric distribution grid transformation projects pursuant to § 56-585.1 A 6 of the Code of Virginia, July 24, 2018.

about vulnerabilities created through third-party vendors and suppliers is growing. In AEP's 2018 Corporate Accountability Report, the company warned of the extent for possible cybersecurity breaches in a modern grid and highlighted the risk created by cloud-based services:

> *New threats and security risks for the electric power grid are constantly emerging as we continue to connect a greater variety of internet-connected devices also referred to as the Internet of Things (IoT). This includes sensors, routers, drones and smart devices that are essential to a modern grid, 24/7 business transactions and data transfers. New mobile apps and services that we develop or procure for customers and increasing reliance on cloud-based programs will increase external connectivity to our network, creating new entry points for potential attackers and posing new challenges for grid security. It is up to each utility to be prepared to contain and minimize the consequences of cyber and physical security incidents.*[372]

Subsequently, in AEP Ohio's 2019 Grid Architecture Status report, the utility expressed concern about third-party security processes and policies:

> *Breaches can come from anywhere, even a trusted contractor connecting to the AEP Ohio network.... AEP Ohio is gaining insight from a working group established in 2018 to vet IoT technology that would be, or is already, in place to ensure better security against cyber risks. The goal is to align business units with consistent processes and policies to ensure security across the enterprise.*[373]

Management of the interface between utility-controlled grid services and grid services provided by third-party vendors or built on top of third-party networks will become increasingly important as the number of services and connections surge. Any discussion of the modernization of the grid should include the risks and opportunities created by expanding the number of parties providing and taking services from the grid.

ELEMENT THREE: DESIGN THE PROCESS TO MAXIMIZE EFFICIENCY AND COLLABORATION

The third element of incorporating cybersecurity into grid modernization efforts is to design the process in a manner that maximizes efficiency and encourages collaboration. Grid needs change, new issues arise, new information becomes available, and the best-made plans become outdated. A well-designed process will efficiently deploy resources while maintaining the flexibility to adapt to changing conditions. That flexibility can come from process design or by a willingness to shift course when circumstances change. This report identifies four steps to creating a flexible and functional process.

372 AEP, 2018 AEP Corporate Accountability Report, 2018 http://www.aepsustainability.com/sustainability/reports/docs/2018-AEP-Corporate-Accountability-Report.pdf at 21.

373 AEP Ohio, PowerForward Initial Assessment Report, April 1, 2019 http://dis.puc.state.oh.us/TiffToPDf/A1001001A19D01B65355J05032.pdf at 25-26.

The first step is the setting of the objectives, goals, and policies that will drive the grid modernization effort. As will be shown in the examples to follow, clearly defined objectives and goals, even when broadly scoped, give shape to the process and instruction to all participating parties. This is the point when all levels of government and the commission can contribute their expertise and exercise their strengths. All parties should be involved, whether it is a governor's office setting out goals, or the legislature providing resources and dictating schedules, or the utility commission using its institutional capacity. Additionally, stakeholders should have an opportunity to participate in all aspects of the process.

The second step is to give the utility commission management of the process. The decision to initiate a grid modernization docket can have different origins and legislatures and governors can provide substantive direction, but the organization of the process should be given to the utility commission. That is where the expertise lays. For example, it is the commission that is best positioned to determine whether to expand existing dockets to consider grid modernization issues or if a new docket is warranted.

The third step is to build the necessary supporting structure for the grid modernization effort. The other sections of this report discuss protecting critical infrastructure confidential information, incentivizing investment with alternative rate mechanisms, adapting reporting and audit processes to enhance information flows, and deploying metrics programs to monitor utility performance. A comprehensive grid modernization program will knit together these distinct elements to produce a functional and flexible process.

The fourth step is to be willing to change. Grid needs will change as new information becomes available. Every day produces new information on cybersecurity vulnerabilities and threats. Due to the length of the time required to complete a grid modernization docket, it is inevitable that technological and policy changes will occur. When change occurs, be able to reset the process based upon newly available knowledge.

State Examples

The following examples highlight how states are acting to build cybersecurity into ongoing and new grid modernization efforts. The examples describe how governors, legislatures, and utility commissions have assumed leadership roles and how they have used their respective powers to create the conditions for grid modernization efforts that are inclusive of cybersecurity.

NEW HAMPSHIRE

New Hampshire's grid modernization process highlights the interplay between the governor, legislature, and utility commission. The process gave space for investigating, learning, and acting on the issues. Most importantly, the grid modernization effort could evolve. Over the length of the process, the attention given to cybersecurity grew to reflect the emergence of heightened concerns about system vulnerabilities.

Initiating the Process

On June 5, 2013, the Governor of New Hampshire signed S.B. 191 establishing the State Energy Advisory Council and directing it to work with the Office of Energy and Planning

to develop a 10-Year Energy Strategy.[374] The Strategy, published in 2014, contained a singular mention of cybersecurity – indicating that it is important to have a modern and resilient grid to protect against the growing threat of physical and cyber-attacks.[375] In 2015, the governor signed H.B. 614, which implemented the goals of the Strategy.[376] One of the statutory provisions required the New Hampshire Public Utility Commission to open an investigative docket into grid modernization.[377] The Staff were directed to examine proceedings in other states, to look at materials produced by the federal government, and to ensure that policies and regulatory mechanisms allowed for new technologies to be adopted.[378]

Scoping the Process

In July 2015, the Commission issued the order opening the grid modernization investigative docket.[379] The investigative docket was used to scope the substantive and procedural elements of the process that would be used to initiate a grid modernization program in New Hampshire. Stakeholders were afforded the opportunity to learn about grid modernization and to explore how grid modernization might work in New Hampshire.[380] The Commission solicited comments on the scope of grid modernization proceedings; looked into the work of other state's grid modernization efforts; and initiated a Working Group to solicit input from distribution companies and other stakeholders.[381]

On March 20, 2017 the Working Group submitted the Grid Mod Working Group Report and its recommendations to the Commission. The recommendations were intended to the guide the Commission in the next steps of the grid modernization process.[382] For example, to identify opportunities to build on existing processes, the Working Group recommended that the Commission prepare a list of related dockets that contain grid modernization elements.[383] The Working Group advised that a cybersecurity plan should be part of each utility's grid modernization plan, but left a series of questions for further study including types of data that would be included in the plans, filing requirements, and integration with other planning processes.[384]

374 New Hampshire, S.B.191-FN-A, 2013http://www.gencourt.state.nh.us/legislation/2013/SB0191.pdf.

375 New Hampshire Office of Energy & Planning, New Hampshire 10-Year State Energy Strategy, September 2014 https://www.nh.gov/osi/energy/programs/documents/energy-strategy.pdf at 17.

376 New Hampshire, H.B. 614-FN, 2015 https://legiscan.com/NH/text/HB614/id/1255159/New_Hampshire-2015-HB614-Chaptered.html.

377 New Hampshire HB 614-FN, § 219:1(I), 2015. ("The public utilities commission shall open a docket on electric grid modernization on or before August 1, 2015.").https://legiscan.com/NH/text/HB614/id/1255159/New_Hampshire-2015-HB614-Chaptered.html

378 New Hampshire Office of Energy & Planning, New Hampshire 10-Year State Energy Strategy, September 2014 https://www.nh.gov/osi/energy/programs/documents/energy-strategy.pdf at 21-22.

379 New Hampshire Public Utilities Commission, IR 15-296, Investigation into Grid Modernization, Order of Notice July 30, 2015 https://www.puc.nh.gov/Regulatory/Docketbk/2015/15-296/INITIAL%20FILING%20-%20PETITION/15-296%202015-07-30%20ORDER%20OF%20NOTICE.PDF.

380 *Id.* at 2.

381 *Id.* at 2.

382 Grid Modernization Working Group, Report to the New Hampshire Public Utilities Commission, Grid Modernization in New Hampshire, March 20, 2017, https://www.puc.nh.gov/Regulatory/Docketbk/2015/15-296/LETTERS-MEMOS-TARIFFS/15-296_2017-03-20_NH_GRID_MOD_GRP_FINAL_RPT.PDF at 5.

383 *Id.* at 32.

384 *Id.* at 10.

While the Working Group developed a list of questions, it was the Commission Staff that were tasked with providing answers. Consequently, the NHPUC Staff turned to outside resources to determine their next steps.[385] Staff reviewed other state dockets on grid modernization and attended trainings by NECPUC and the DOE.[386] The trainings were based on DOE's Office of Electricity Delivery & Energy Reliability's Modern Distribution Grid report.[387] The Staff noted that "DOE's approach for distribution planning and grid operation links investments to stated objectives and goals while building a platform for the distribution system that will facilitate the integration of DERs."[388] The trainings helped staff create a "methodological approach for the development of a grid mod framework that aligns utility investment plans with grid mod objectives."[389]

Integrate Grid Modernization with Other Processes

In February 2019, the finalized Staff Grid Modernization Report was released.390 In the Grid Modernization Report, Staff identified several related dockets and centered in on the existing least cost integrated resource plan (LCIRP) requirement as the preferred option for combining with grid modernization. The Staff Report recommended combining the LCIRP and the grid modernization into an Integrated Distribution Plan (IDP). The IDP would contain a 10-year roadmap, a 5-year capital investment plan, and 5-year operational expense plan.[391]

This alignment would bring forth existing filing requirements of the LCIRP process which includes an obligation to provide:

> *[a]n assessment of distribution and transmission requirements, including an assessment of the benefits and costs of "smart grid" technologies, and the institution or extension of electric utility programs designed to ensure a more reliable and resilient grid to prevent or minimize power outages, including but not limited to, infrastructure automation and technologies.*[392]

The Staff recommendations captured the split and the balancing between data privacy and grid operations. Per the Staff recommendation, the IDP would contain the "utility's cyber security strategy, privacy policies and standards."[393] Also, system management was differentiated from customer data management, indicating that the cybersecurity

385 New Hampshire Public Utilities Commission, IR 15-296 Investigation in Grid Modernization, Staff Recommendations on Grid Modernization, January 31, 2019 at 8.
386 *Id.* at 8.
387 US Department of Energy, Office of Electricity Delivery & Energy Reliability, Modern Distribution Grid, Volume I: Customer and State Policy Driven Functionality, Version 1.1, March 27, 2017; Volume II: Advanced Technology Maturity Assessment, Version 1.1, March 27, 2017; Volume III: Decision Guide, June 28, 2017. https://gridarchitecture.pnnl.gov/modern-grid-distribution-project.aspx.
388 New Hampshire Public Utilities Commission, IR 15-296 Investigation in Grid Modernization, Staff Recommendations on Grid Modernization, January 31, 2019 at 8.
389 *Id.* at 7.
390 *Id.*
391 *Id.* at 15.
392 RSA N.H. Title XXXIV § 378:38.
393 *Supra* note 388 at 75.

protection needs of information technology and operational technology warranted individualized considerations.[394]

Confidential information protections would be baked into the process. Utilities would be prohibited from including information in the IDP that would compromise their security plans.[395] However, these restrictions are balanced by the requirement that a utility must demonstrate, at a high level, in its implementation plan that it is addressing cyber security and privacy throughout its system with a particular focus on distributed energy resources (DERs).[396]

The Staff Report also contains a recommendation for evolving reporting requirements and for utility self-assessment. In the Report, Staff noted that DER technologies such as energy storage and generation such as wind or solar would require a higher level of cybersecurity than customer data management. Staff recommended the IDP include:

> *(a) A list of all anticipated vulnerabilities in the system, and a proposed mitigation strategy; and*
>
> *(b) Evidence that each utility is monitoring and implementing the latest National Institute of Standards and Technology (NIST) standards and cyber security framework by addressing the following: Authentication and identity; Self-assessing cybersecurity risk; Managing cybersecurity within the supply chain; and Vulnerability disclosure.*[397]

Staff also recommended that utilities consult NARUC's 2017 Primer on Cybersecurity for State Utility Regulators when developing their plans.[398]

Evolving the Process

Fleshing out the mechanics of the IDP is an ongoing process that will require additional research. The Staff Report suggested forming working groups, including a Cybersecurity working group.[399] The working groups could draw "on the experience of neighboring states in the establishment of a business-to-business collaborative requiring that all entities that interface with utility systems have adequate cyber protections in place, in addition to those already established by the utilities themselves."[400]

The flexibility of the approach used to develop the grid modernization plans and their mandated content allowed the Commission to adapt to changing circumstances. Over the six years that the grid modernization program has been developing, the knowledge and familiarity with cybersecurity issues increased with every subsequent report or filing. Importantly, the process is ongoing as the Commission is still determining the procedural elements and substantive requirements that will constitute the IDP process.

394 *Supra* note 388 at 75.
395 *Supra* note 388 at 75.
396 *Supra* note 388 at 75.
397 *Supra* note 388 at 75.
398 *Supra* note 388 at 76.
399 *Supra* note 388 at 76.
400 *Supra* note 388 at 76.

HAWAII

Hawaii's grid modernization process is driven by changing grid dynamics. High levels of DER penetration and Hawaii's adoption of a 100% RPS by 2045 were the impetus for electric utilities, stakeholders, and the Hawaii Public Utility Commission to begin discussions of what a modern electric grid would look like, and the appropriate way to invest in that grid.[401]

Hawaii's grid modernization effort demonstrates the value of clear directions and guidance and the willingness to restart a process when it does not produce a product commensurate to the challenge presented. The development of the Hawaiian Electric Companies'[402] (HECO) Grid Modernization Strategy shows how a utility commission can provide direction to utilities and can craft a process that facilitates stakeholder participation. Strong guidance from the Commission helped shape evaluative processes that could produce a proactive and progressive plan. Hawaii's grid modernization effort also benefited from a process that created manageable chunks of investigation and implementation. The flexibility and adaptability derived from this choice allow for an efficient deployment of resources to learn about an issue and to subsequently act upon the issue.

Application Dismissal and Commission Guidance

In March of 2016, HECO filed a joint application to fund a Smart Grid Foundation Project Standards.[403] In January 2017, the Commission dismissed the application without prejudice on the grounds that the application lacked the specificity necessary to meet the gravity of revisioning the grid, particularly changing technologies, integrating DER growth, and the role of non-utility energy service providers.[404] The Commission ordered HECO to submit a "detailed, scenario-based Grid Modernization Strategy" based on rigorous stakeholder and industry expert input.[405]

To address a complicated issue like grid modernization, a process was needed that allowed for extensive stakeholder and industry expert input. The Commission identified that the existing process for submitting the Grid Modernization Strategy, as defined per the guidelines of General Order No. 7, (G.O. 7) was limiting because of its prescribed format.[406] Therefore, the Commission sought to create an alternative process with more flexibility to give sufficient time to discuss issues. Additionally, in its dismissal of HECO's original application, the Commission provided guidance on areas that should be addressed in the Grid Modernization Strategy including "[h]ealth, cybersecurity, data access and privacy."[407] The act of splitting cybersecurity and data access and privacy ensures that information and operational technology would receive individualized attention.

401 Grid Modernization Laboratory Consortium (GMLC), State Engagement in Electric Distribution Planning, December 2017. https://epe.pnnl.gov/pdfs/State_Engagement_in_Electric_Distribution_System_Planning_PNNL_27066.pdf at 2.1.

402 The Hawaiian Electric Companies (HECO) is comprised of Hawaiian Electric Co., Inc., Hawaii Electric Light Co. Inc., and Maui Electric Light Co., Ltd.

403 Hawaii Public Utilities Commission, Application of Hawaiian Electric Company, Inc., Hawaii Electric Light Company Inc., and Maui Electric Company, Limited, Exhibits A-I; Verification; and Certificate of Service, March 31, 2016.

404 Hawaii Public Utilities Commission, Order No. 34281, Dismissing Application without Prejudice and Providing Guidance for Developing a Grid Modernization Strategy, January 4, 2017 at 4.

405 *Id.* at 10-11.

406 *Id.* at 4.

407 *Id.* at 8.

The Commission offered significant guidance to HECO for the revision process. First, it presented multiple questions to guide the utility in revising its Strategy. Second, it reiterated HECO would need separate information and operational technology standards that would protect the "customer's privacy and the electric system's security."[408] Furthermore, the standards would be expected to evolve in response to changing technology and customer needs.[409] Lastly, HECO was instructed to tackle the question of how grid architecture should be "optimized to address the elements of interoperability, cybersecurity, flexibility, and adaptability."[410] The Commission framed this question under the objective of proactivity. How could the grid architecture be proactively designed "versus passively allowing the grid to evolve in a bottom-up manner and waiting to see what emerges."[411]

Lastly, the Commission provided definitions for HECO in its resubmission of its Grid Modernization Strategy. The Commission's definition of grid architecture covers third-party vendors and suppliers by encompassing the entire scope of grid hardware, including what was controlled by utilities and "many elements that exist outside the utility but that interact with the grid, such as buildings, DER, and microgrids."[412] The Commission defined interoperability as "seamless, end-to-end connectivity of hardware and software from the customers' appliances all the way through the transmission and distribution system to the power source, enhancing coordination of energy flows with real-time flows of information and analysis."[413] This definition captures most, if not all, of the potential attack surface.

Revised Strategy

In August 2017, HECO published the final draft of its Strategy. The draft Strategy contained significantly more detail in multiple areas including operational cybersecurity which was broken in two parts, Grid-Side Cybersecurity and DER Cybersecurity.[414] The split acknowledges the different regulatory regimes for utility-controlled assets and customer or third-party controlled assets. In Grid-Side Cybersecurity, HECO acknowledged that the "development of a more proactive advanced persistent threat identification process" would be a critical element in elevating its cybersecurity posture. HECO also stated that it drew upon industry best practices developed and/or catalogued by NIST, DOE, EPRI, and NARUC.[415]

HECO's approach meets the Commission's instructions that cybersecurity protections will need to be flexible and evolving. For example, in the DER Cybersecurity section, HECO

408 *Id.* at 19.
409 *Id.* at 19.
410 *Id.* at 57.
411 *Id.* at 55.
412 *Id.* at 54.
413 Hawaii Public Utilities Commission, Order No. 34281 at 56. Citing to GridWise Architectural Council Policy Team, "Introduction to Interoperability and Decision-Maker's Interoperability Checklist Version 1.0," at 1 http;//www.gridwiseac.org/pdfs/gwac decisionmakerchecklist.pdf.
414 The DER Cybersecurity subsection was adapted from DOE, Modern Distribution Grid Report: Volume III, 2017.
415 The Strategy listed National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, DOE Energy Sector Cybersecurity Framework Implementation Guidance, DOE Risk Management Process, EPRI's Risk Management Guide, and the National Association of Regulatory Commissioners (NARUC) Cybersecurity Primer. Hawaiian Electric Companies, Modernizing Hawai'i's Grid for Our Customers, June 30, 2017 at 77.

expressed concern about the lack of visibility into DERs and inverters. HECO stated there is "no cybersecurity requirement or oversight on the aggregated DERs/inverters," which constitutes a "significant gap" with "very material consequences on overall electric system security as DER adoption becomes a large portion of system resources."[416] This statement reflects the Commission's all-encompassing definition of grid architecture, and echoes the concerns about attack surfaces that are beyond the Commission's regulatory authority.[417]

From Application to Implementation

A shift in scope and focus occurred as the process moved from discussing goals and objectives to implementing them. In February 2018, the Commission conditionally accepted Phase 1 of HECO's Grid Modernization Strategy.[418] The approval of HECO's Grid Modernization Strategy was followed by the opening of a docket on how to implement the Strategy.[419] HECO filed its Grid Modernization Strategy Phase 1 Application to the Commission pursuant to Paragraph 2.3.g.2 of G.O. No.7,[420] the standard that had been previously set aside to allow the development of the Grid Modernization Strategy. The Application focused on a limited number of technologies to be installed over a defined time span, an implementation that could be evaluated under existing, routine commission practices. Allowing for the Strategy to be developed in a unique process, but implementation of the Strategy to be conducted under regular practices allows the Commission to direct resources in a manner that is efficient and matches the depth of the issue under discussion.

OHIO

The Public Utility Commission of Ohio's PowerForward initiative demonstrates how the form and function of a grid modernization effort can be collaboratively developed through stakeholder consultation. The open format of the early development stages gave space to explore and define the different components of cybersecurity. Additionally, the PowerForward process paid special attention to addressing the security risks connected to sharing utility cybersecurity plans with the Commission.

Scoping the Process

In April 2017, the Commission began its PowerForward initiative for the purpose of exploring how the distribution system can be improved through innovation to provide benefits to all Ohioans.[421] Work on PowerForward was divided amongst three phases:

416 Hawaiian Electric Companies, Modernizing Hawai'i's Grid for Our Customers, June 30, 2017 at 80.

417 Electric Energy Online, From Research to Action: How to Navigate Existing Cyber Security Risk Management Guidance, https://electricenergyonline.com/energy/magazine/840/article/From-Research-to-Action-How-to-Navigate-Existing-Cyber-Security-Risk-Management-Guidance.htm.

418 Hawaii Public Utilities Commission, Docket 2017-0226, Decision and Order No. 35268, Instituting a Proceeding Related to The Hawaiian Electric Companies' Grid Modernization Strategy, February 7, 2018.

419 Hawaii Public Utilities Commission, Docket 2018-0141.

420 Hawaii Public Utilities Commission, Docket 2018-0141, Decision and Order No. 36320, For Approval to Commit Funds in Excess of $2,500,000 for the Phase 1 Grid Modernization Project, and Related Requests, March 25, 2019 at 2.

421 Public Utility Commission of Ohio, "PowerForward, A Roadmap to Ohio's Electricity Future." August 29, 2018 https://www.puco.ohio.gov/industry-information/industry-topics/powerforward/powerforward-a-roadmap-to-ohios-electricity-future/ at 4.

Phase 1 – A Glimpse of the Future; Phase 2 – Exploring Technologies; and Phase 3 – Ratemaking and Regulation.[422] Phase 3 included an investigation into how cybersecurity threats and protections would change as the grid modernized. Hundreds of hours of meetings and presentations were conducted over multiple months, leading up to the Commission's August 2018 release of its recommendations for grid modernization, *PowerForward: A Roadmap to Ohio's Electricity Future (Roadmap)*.[423]

Cybersecurity Recommendations

The Roadmap set forth a series of recommendations for how to proceed in grid modernization efforts including recommendations on cybersecurity. The recommendations address reducing security risks, increasing the information available to the Commission, and how to manage emerging issues. The Roadmap also acknowledged that cybersecurity risks are increasing due to changes in technology, growing use of cloud-based services, and the proliferation of customer and third-party access to those systems.[424]

The Commission took deliberate action to limit its oversight as a means of improving the security of the distribution grid. The Commission stated it would decline to develop and approve cybersecurity-specific reporting requirements for utilities.[425] The Commission argued that it could meet its obligation to ensure a safe and secure supply of energy without compromising grid security. It wrote "[b]y limiting the Commission's oversight of each utilities' annual report and PowerForward filings, the Commission intends to satisfy its regulatory goals while eliminating the inherent risks that could arise if the Commission reviewed each EDU's cyber policies and procedures."[426] The Commission's actions were driven by the concern that overregulation would reveal specific vulnerabilities in the system and cause delay that could leave a utility open to attack while waiting on government approval. This concern outweighed the risk of an attack for lack of a sufficiently regulated system.[427] Instead, the Commission suggested that each utility be required "to confirm that they in fact have a plan to sufficiently address cybersecurity concerns that is consistent with industry best practices, similar to the requirements for emergency plans and coordination for restoration of electric service contained in Ohio Adm.Code 4901:1-10-08."[428] Each utility is required to submit an annual confirmation of "adequate cybersecurity planning" in a separate docket unless the measures are specific to protecting PowerForward investments.[429, 430]

To facilitate deeper discussions, the Commission spun off cybersecurity discussions into a different forum. On February 27, 2019, the Commission issued an order adopting the findings of the Roadmap and directing electric distribution utilities to file grid architecture

422 *Id.* at 10-11.
423 Public Utilities Commission of Ohio, PUCO directs electric utilities to file grid modernization reports, February 27, 2019, https://www.puco.ohio.gov/media-room/media-releases/puco-directs-electric-utilities-to-file-grid-modernization-reports/.
424 *Supra* note 421 at 32.
425 *Supra* note 421 at 32-33.
426 *Supra* note 421 at 33.
427 *Supra* note 421 at 32-33.
428 *Supra* note 421 at 33.
429 Public Utilities Commission of Ohio, Case No. 18-1596-EL-GRD, Finding and Order, In the Matter of the PowerForward Distribution System Planning Workgroup, February 27, 2019 at 5.
430 *Supra* note 421 at 33.

status reports by April 1, 2019.[431] In that same order, the Commission noted that multiple utilities raised concerns about addressing cybersecurity their grid architecture status reports. Utilities were concerned about the risks created by providing information in a public docket and what content should be included in the upcoming cybersecurity plan filings.[432] The Commission responded that it would open a separate cybersecurity docket would be opened, as per the recommendations made in the PowerForward Report, to fully flesh out the concerns and the solutions to the concerns.[433]

The grid modernization process developed by the Commission is an open process that will continue to solicit information and provide feedback. To facilitate continued engagement, the Commission opened a series of dockets to house the activities of the PowerForward Collaborative, the Distribution System Planning Workgroup (PWG) and the Data and Modern Grid Workgroup (DWG).[434] The intention of the dockets is to allow stakeholders an opportunity to see the project forward with Staff and participate in its evolution.[435]

Conclusion

Grid modernization is happening right now. The question, as posed by the Hawaii Public Utilities Commission, is will it be a process that is shaped by legislators and regulators or will it be a process that develops without structure or guidance. Grid modernization dockets are an opportunity to build cybersecurity into the next evolution of the grid. Active engagement by utility commissions can create adaptive and flexible processes that can shift in accordance with available knowledge. Active engagement will ensure that critical issues such as confidential information protections and third-party vendors are addressed early and completely. The changing grid will create cybersecurity risks, but it also represents an opportunity to install practices and policies now that can meet future challenges.

431 *Supra* note 429.
432 *Supra* note 429 at 3, 5.
433 *Supra* note 429 at 6.
434 Public Utilities Commission of Ohio, PUCO establishes PowerForward Collaborative, Oct. 24, 2018 https://www.puco.ohio.gov/media-room/media-releases/puco-establishes-powerforward-collaborative1/. On October 23, PUCO opened a collaborative docket for SmartGrid and Advance Metering Applications per the PowerForward policy (18-1595-EL-GRD), and issued an order establishing the PowerForward Collaborative, and its subgroups. The distribution system planning subgroup was docketed at 18-1596-EL-GRDN. The Data and Modern Grid Workgroup was docketed at 18-1597-EL-GRD.
435 *Id.*

SECTION 7
SUMMARY

THE CYBER THREATS TO OUR ELECTRIC DISTRIBUTION GRID are growing in frequency and potency. Securing the grid against attack and preparing to respond to an attack and its aftermath, will take tools and techniques that enhance information flow between utilities and their regulators, assess and direct utility performance, and facilitate targeted investment.

This report began with a detailed discussion of how to define and protect critical infrastructure information as it is through this protection that the potential of all the other grid improvement tools are unlocked. Management and operations audits, cybersecurity reporting requirements, resiliency metrics, and grid modernization dockets can improve decision-making, but only if the information flows are trusted and secure. The report highlighted essential elements that must be part of the definition of critical infrastructure, including the difference between information technology and operational technology.

The paths by which tools to improve the grid are developed and implemented are also important. By understanding the origins of the tool, we see that governors' offices, legislatures, and utility commissions each have a critical role to play in securing the grid. Most of the tools and techniques described in the report are implemented at the utility commission level, but they arise from action started by a commission, legislature, or governor. Regardless of where the originating action is taken, the expertise of a utility commission is critical to framing out and applying the tools.

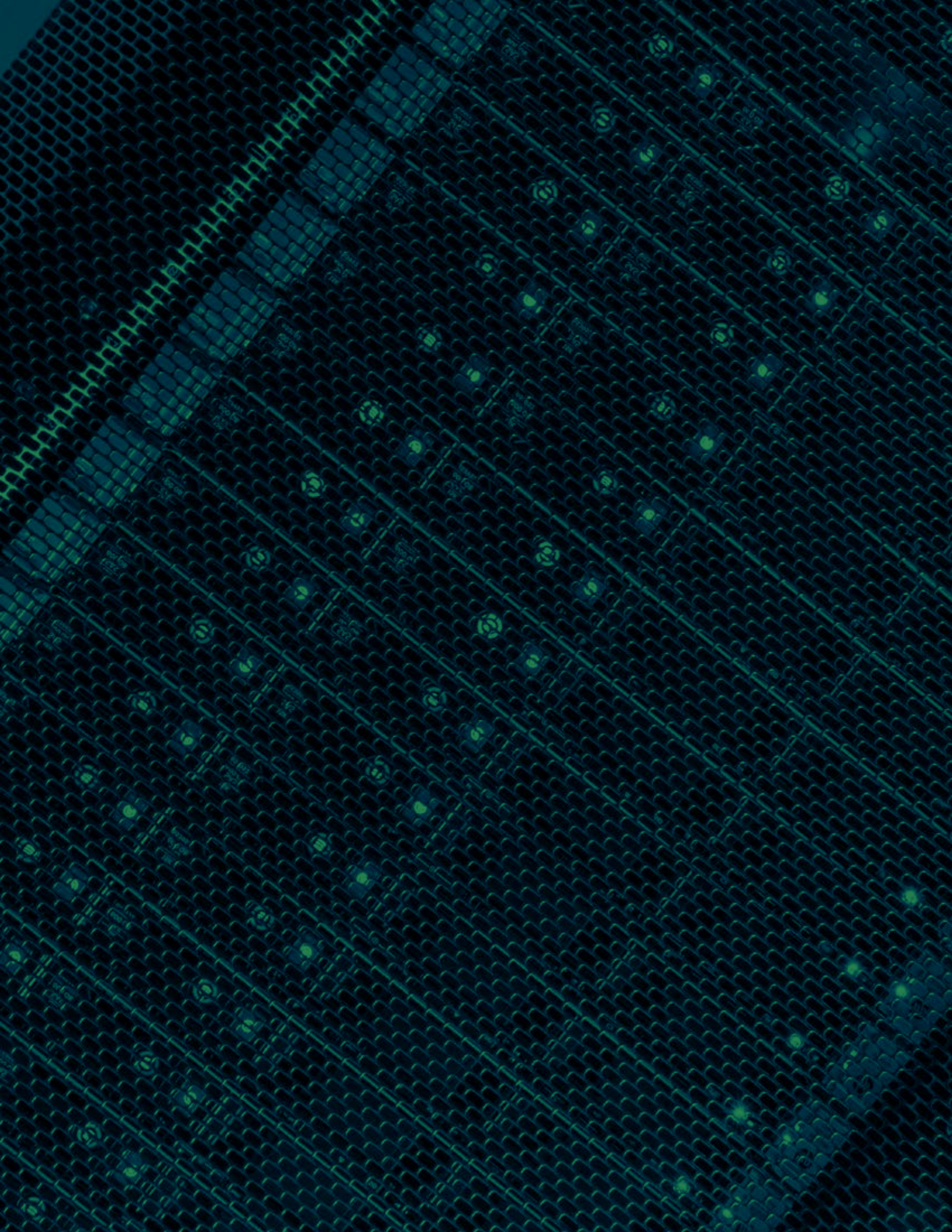
The report also looks at the critical need to incentivize investment in cybersecurity protections. Regulatory lag is a growing concern for utilities seeking to invest in

cybersecurity. The use of an alternative rate mechanism could incentivize needed investment, but its use must be balanced with protections for the ratepayer. Multiple design options that properly weigh the benefits and costs of alternative rate mechanisms are presented herein.

The information asymmetries that exist between utilities and their regulators also exist utility-to-utility. Breaking down these barriers is crucial to securing the grid. Existing audit and reporting processes can do that, and they can be readily tailored to the institutional capacity of utilities and their regulators.

The procedures and processes highlighted in the report focus not only on achieving best practices but doing so on an on-going basis. Continuous improvement is critical as new threats emerge and new vulnerabilities are identified. Grid security today is only as good as the last improvement made.

Lastly, the report presents several examples and options for resolving barriers that limit our preparedness and responsiveness. Recognizing that the needs and abilities of every state vary, the diversity of options is a strength as each state can take action that fits their individual circumstances and resources. It is important to note that all actions are valuable since every action taken is a step towards improving the cybersecurity of the distribution grid. Improving the cybersecurity of the distribution grid will take time, and considerable, sustained effort, but the time to act is now.



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

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

ADAM MCGOVERN is a 2019 Masters of Energy Regulation and Law graduate.

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

AUSTIN SCARBOROUGH is a 2021 JD/Masters of Energy Regulation and Law candidate.

KRISTEN ZWEIFEL is a 2020 Accelerated JD candidate.

MARK JAMES is an Adjunct Professor of Law at Vermont Law School and 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