FEBRUARY 2017

PUBLIC UTILITIES FORTNIGHTLY

"In the Public Interest"

Susan Story, Tanuj Deora
Barry Worthington, Moody's
Seven Northeast Utility Execs
2016 Author/Interview Index

Cybersecurity

Opportunities & Challenges for Regulators

Part I of their article on page 38

Nakhia Crossley
IL Commerce Commission

Caitlin Shields
Wilkinson Barker Knauer LLP

Commissioner Sherina Maye Edwards
IL Commerce Commission

Anne McKeon
IL Commerce Commission

In PUF, Impact the Debate

PUBLIC UTILITIES FORTNIGHTLY
"In the Public Interest"

February 2017 • Volume 155, No. 2

In 2017, organizations over a hundred employees will be converted to site licenses.

Cover photographer: Michael R. Herkes, MRH MultiMedia.

Cybersecurity

Opportunities and Challenges for State Utility Regulators

PART I

By Commissioner Sherina Maye Edwards, Illinois Commerce Commission and Caitlin Shields

With Anne McKeon and Nakhia Crossley

Public utility companies touch nearly every person's life on a daily basis through the transmission, distribution and consumption of gas, electricity and water. They also increasingly rely on networked technology to conduct their business.

However, attackers are acting faster, becoming more sophisticated, and getting more strategic in their attacks, including their abilities to navigate the increased complexity and connectivity of critical infrastructure systems.

The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) recently reported that the energy sector has become the biggest cybersecurity target in America. The ICS-CERT 2015 Incident Response Statistics Report accounted for two hundred ninety-five energy sector-related incidents last year alone.

Last year, a Lloyd's of London report found that a widespread attack on the U.S. grid could lead to an economic loss ranging from two hundred forty-three billion up to a trillion dollars. Fallout could include a rise in mortality rates, a decline in trade, disruption to water supplies and transportation chaos.

As utility infrastructure becomes increasingly automated, ensuring the security of critical energy infrastructure is becoming a major concern. Not just for the companies that own and operate such assets, but also for the local, state and federal regulators tasked with ensuring the safety, reliability and cost-effectiveness of the services delivered as well.

While state commissioners have not traditionally regulated this area, many are now grappling with the proper role to play. This article examines the evolving role of state regulators in addressing cybersecurity in the energy sector.

It highlights the importance of developing state regulatory processes that promote efficiency, maintain confidentiality, consider affordability and incentivize investment, while ensuring both the cost-effectiveness and security of utility infrastructure.

Where Are We Now?

While some of the first cyber attacks on infrastructure date back to the 1980's, the Stuxnet worm is widely considered to be the most sophisticated contemporary attack. In 2010, it was discovered that the Stuxnet worm had targeted industrial control systems in Iran by installing a highly specialized malware designed to target SCADA systems that controlled industrial facilities such as power plants, dams and waste processing systems.

The DHS reported that the energy sector has become the biggest cybersecurity target in America.

This allowed attackers to take control of these systems. Stuxnet will likely be used as a blueprint for similar malware in the future.

At the end of 2015, Ukraine experienced a devastating attack on its grid that left thousands of people without power for six hours in the middle of the winter. According to Robert Lee of the SANS Institute, "Despite what's been said by officials in the media, every bit of this is doable in the U.S. grid."

He also noted that recovery in the U.S. could be more difficult because many systems in the U.S. are fully automated, which means switching to manual control is not an option.

In 2015, The Wall Street Journal discovered that Iranian attackers had gained access to the flood gates of the Bowman Avenue Dam near Rye Brook, New York two years before. According to a former official, it was not a sophisticated intrusion, but a test by the hackers to gauge accessibility to the system.

The 2016 Verizon Data Breach Digest summarized several high profile cybersecurity incidents. One was a breach of a water utility, the name of which was not publicized. The report states that two and a half million customer records were compromised.

The hacker was able to manipulate the water flow and distribution rates as well as the amount of chemicals used for water treatment. A breach of this type and magnitude could have triggered a severe state of emergency, but thankfully this was another instance of cyber espionage rather than an attack.

Sherina Maye Edwards is a Commissioner on the Illinois Commerce Commission. She takes an interest in electric reliability, pipeline safety and critical infrastructure issues. Commissioner Edwards earned a J.D. from Howard University School of Law.

Caitlin M. Shields is an Associate at Wilkinson, Barker, Knauer, LLP. She focuses her practice on energy and environmental regulation. Caitlin earned her J.D. at the University of Denver Sturm College of Law.

Nakhia C. Crossley is legal counsel and policy advisor to Commissioner Edwards. Nakhia provides analysis and research on the regulation of the energy, telecommunications, water, and transportation industries. Nakhia earned her J.D. from Thomas Jefferson School of Law.

Anne McKeon joined the Illinois Commerce Commission as a legal and policy advisor to Commissioner Sherina Maye Edwards in August 2015. Anne earned her J.D. from Notre Dame Law School.

Several recent physical attacks on U.S. infrastructure are particularly alarming. In 2013, attackers conducted a sophisticated physical attack on Pacific Gas & Electric's Metcalf substation outside Silicon Valley. The attack took out seventeen electric transformers and required twenty-seven days to complete repairs.

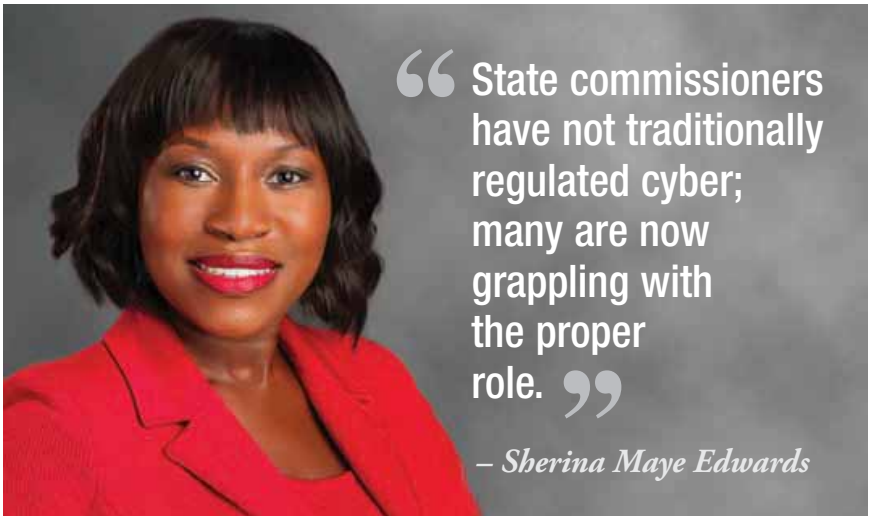
Then-FERC Chairman Jon Wellinghoff described the attack as "The most significant incident of domestic terrorism involving the grid that has ever occurred in the U.S."

A similar physical attack occurred in October 2016 in Utah, when someone with a high-powered rifle fired several shots and disabled a substation owned by Garkane Energy Cooperative. This led to a daylong power outage for about thirteen thousand customers.

According to Navigant energy director Brian Harrell, "Electric infrastructure continues to be vulnerable to firearms attack. We must assume that at some point in the future a North American utility will suffer from a planned and coordinated attack."

In hindsight, key vulnerabilities that allowed Stuxnet to succeed included insecure software, improper information technology, security management and insufficient personnel training.

On the other hand, the PG&E and Garkane incidents reveal the physical vulnerabilities inherent in large, critical infrastructure. That infrastructure often sits in plain sight alongside the streets we drive, the offices we work in, or the paths we walk.



The energy industry has taken several steps to combat cyber attacks on critical utility infrastructure. On July 20, 2006, FERC designated NERC as the entity responsible for developing, monitoring and enforcing compliance with reliability standards for regional entities across the country.

NERC's Critical Infrastructure Protection (CIP) standards address the security of cyber assets that are essential to the reliable operation of the electric grid. By virtue of FERC's limited jurisdiction over the transmission of electricity in interstate commerce, these standards are only required for the utilities that operate the electric grid. They are the only mandatory cybersecurity standards in place across U.S. critical infrastructures.

In 2013, President Barack Obama stressed the importance of increased cybersecurity measures for critical infrastructure in his State of the Union speech and subsequent Executive Order 13636. The executive order establishes a voluntary program to identify incentives for adoption of the cybersecurity framework. It also calls for regulatory agencies to complete a review of existing cybersecurity regulations.

In February 2014, the National Institute of Standards and Technology developed the voluntary NIST Cybersecurity Framework to foster risk and cybersecurity management communications among internal and external stakeholders.

Developed by more than three thousand people from diverse parts of industry, academia and government, the resulting Framework uses a common language to address and manage cybersecurity risk in a cost-effective way.

Many private sector organizations within the utility industry apply these standards with their sector-specific needs in mind. For example, the American Gas Association advocates for its members to participate in cybersecurity discussions at the federal level to ensure that the Framework addresses the concerns of natural gas utilities.

Similarly, the American Water Works Association's Water Utility Council developed a tool to guide water utilities in their use of process control systems. And the Edison Electric Institute offers resources to its members to assist with strengthening cyber defenses. EEI has also developed principles for cybersecurity and critical infrastructure protection.

Opportunities and Challenges

State utility regulators are coming under increasing pressure from constituents and from governors to ensure the safety of the infrastructure they oversee. That presents both opportunities and challenges. While regulators are tasked with the duty of protecting the public interest, many lack the technical background, expertise and resources necessary to manage a utility's cybersecurity policy.

State regulators must respect the various layers of jurisdiction surrounding cybersecurity to ensure their role is not overly burdensome to an industry that is already highly regulated.

Regulators also face the challenges of applying an economic analysis to cyber risk mitigation, ensuring safety of a network interconnected to non-jurisdictional entities and protecting sensitive information. Disclosure laws still vary significantly from state to state.

Jurisdictional Challenges

In the absence of a federal mandate for states to work together, the current patchwork of state regulation can create compliance challenges for utilities and regulators alike. The complexity of multiple standards can lead some companies to focus more on meeting compliance standards than the actual security such standards are intended to advance.

Making such varying standards mandatory may be counterproductive. Utilities could incur greater operational costs to document and audit their programs without necessarily making the consumer more secure.

Not only do requirements differ among states, they also differ among utilities. Because every operating environment is different, it is difficult for regulators to enforce standard compliance requirements.

Smaller utilities, particularly municipal and cooperative utilities, may not have the means to invest in technical controls that might otherwise be required. State regulators often have the authority to regulate and oversee utility cybersecurity programs. However, regulators and utilities must communicate to ensure any compliance mechanisms do not cause inefficiencies.

Though state regulators have not traditionally been involved in overseeing the cybersecurity of critical energy infrastructure, this is beginning to change. State public utility commissions are playing an increasingly important role in determining which cybersecurity measures utilities should be required to implement on the distribution system.

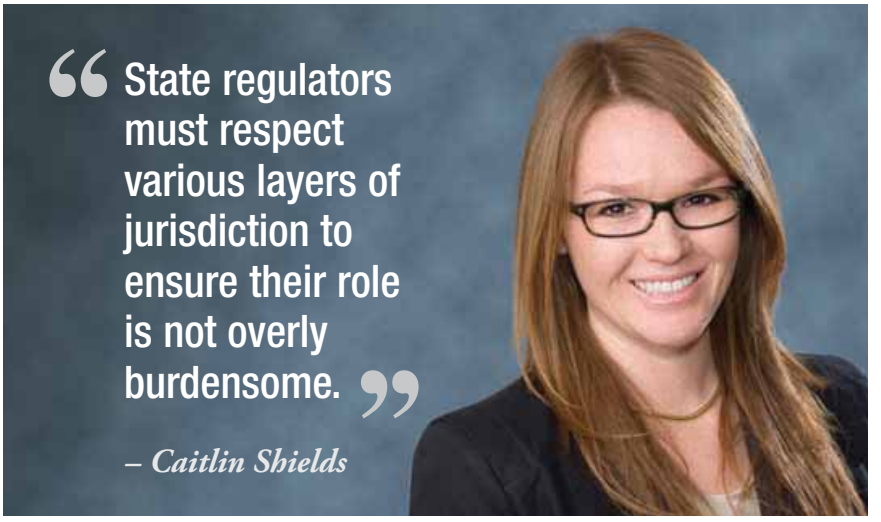
They are also helping to determine which associated costs are prudently incurred, how the costs of these investments should be amortized, and how utilities' cybersecurity programs and preparedness should be audited. And state utility regulators are beginning to develop policies that govern information sharing between utilities, government entities, third-party vendors and the public.

Given the sheer size and complexity of our nation's gas, electric, water and telecommunications infrastructure, regulators at all levels of government face jurisdictional challenges. With so many stakeholders, it can become difficult to tell where overlapping jurisdictional boundaries begin and end. This can also lead to the unintended consequence of gaps in regulatory jurisdiction.

For instance, the federal NERC-CIP standards apply only to the bulk power system, such as transmission providers. However, regulation of investor-owned distribution systems typically falls on state regulators. Additionally, the CIP standards only cover assets that qualify as "critical," which excludes advanced meters and other smart grid technologies that impact reliability, operational safety and customer privacy.

Alarmingly, it is estimated that eighty to ninety percent of grid assets fall outside the scope of CIP standards, indicating the majority of utility critical infrastructure is not subject to any mandatory federal cybersecurity standard. Some argue that these exclusions provide a roadmap for potential attackers to identify and target specific systems and controls and to attack infrastructure.

Other jurisdictional issues arise when utilities have service territories that cross state lines, subjecting them to multiple regulatory regimes. And neither FERC nor state regulators can regulate direct interactions between non-utility service providers and consumers regarding the sale of "smart" products and services, such as electric efficiency analysis and energy management. Reliance on the Internet to conduct this type of business increases vulnerability to malicious software and the potential for service disruption.



In order for state regulators to have a meaningful role, they must collaborate with other state and federal regulators and lawmakers to ensure consistency, efficiency and harmony across jurisdictions. Moreover, it is critical that regulators collaborate closely with utilities to understand the day-to-day challenges they face.

At the same time, duplication of efforts, particularly those related to compliance and reporting requirements, should typically be avoided in order to increase efficiencies. Information sharing and cross-sector collaboration will be essential to addressing these jurisdictional issues.

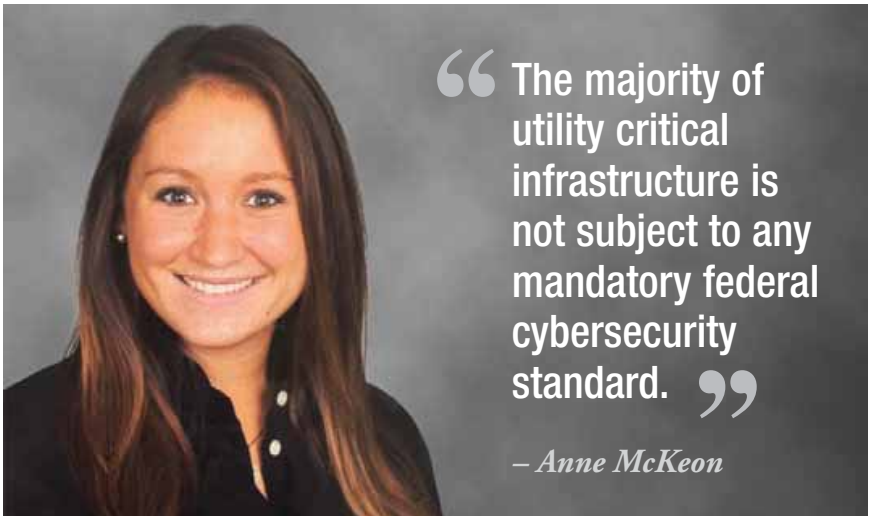
While there is no one-size-fits-all formula, enhancing grid security at local, state and national levels requires a multi-faceted approach. There is a wide array of stakeholders and a mix of voluntary and mandatory compliance standards. In most states, commissions are not required by law to establish cybersecurity standards.

However, many state regulators are increasing their oversight and involvement, using stakeholder working groups, docketed cybersecurity rulemakings, advanced metering infrastructure (AMI) deployment proceedings, rate cases, audits and reporting requirements.

Regulators typically have a wide range of regulatory and enforcement tools available to them. However, it is critical that regulators first develop an understanding of what their regulated entities and other state agencies are already doing in order to develop an effective cybersecurity framework.

There are several examples of state-specific actions. The Pennsylvania Public Utilities Commission (PUC) adopted rules requiring each of its regulated utilities to develop physical security, cybersecurity, emergency response and business continuity plans. To avoid repetitive reporting, the Pennsylvania Commission allows utilities to submit a plan required by another jurisdictional entity in lieu of the state plan.

In 2003, the New York PSC established an Office of Utility Security, which is tasked with monitoring security planning, implementation and performance regarding critical infrastructure protection. Generally, the commission uses existing NERC CIP standards as benchmarks. N.Y. PSC Staff now conducts regular on-site evaluations of utility cybersecurity measures, practices and procedures.



In 2011, the Ohio PUC hosted an emergency tabletop exercise with industry stakeholders. The Ohio Commission has also initiated an audit of Duke Energy Ohio's AMI, sponsored cybersecurity workshops, initiated training sessions for industry stakeholders and solicited comments on how to best address cybersecurity issues.

In 2015, the Missouri Public Service Commission opened a docket to examine cybersecurity and physical infrastructure security issues. It requires verbal reporting of "cybersecurity or infrastructure security events that affect many customers, involve the release of customer proprietary information, or pose a threat to the general public."

In Maryland, as a requirement of utilities' AMI deployment, BGE, PEPCO and Delmarva have provided "basic publicly available information on how the utility is protecting its AMI and the responsible utilities' organization for cybersecurity." The companies are also required to file reports addressing cybersecurity topics.

The New Jersey Board of Public Utilities recently adopted a set of comprehensive cybersecurity requirements for electric, natural gas and water/wastewater utilities. They are directed to create cybersecurity programs that define responsibilities for cyber risk management activities. They must also establish procedures for identifying and mitigating cyber risk to critical systems through risk assessments and cybersecurity training programs.

These examples show varying levels of commission engagement in terms of enacting and enforcing cybersecurity regulations. Some states exercise their authority through informal avenues, while others require formal proof of compliance. Though certain states have created requirements, their methods are not identical to one another. They do not mirror the requirements outlined by the federal government, while other state commissions have yet to address the issue at all.

Cost Recovery

In the case of rate-regulated utilities, regulators must balance the objectives of ensuring service that is safe and reliable yet also cost-effective. Without a framework to determine whether cybersecurity investments actually produce resilience, it becomes difficult for regulators to make prudency findings and authorize recovery through rates. Where bright line standards such as NERC's CIP requirements or state legislation exist, utilities can more readily demonstrate that related cybersecurity investments are prudent.

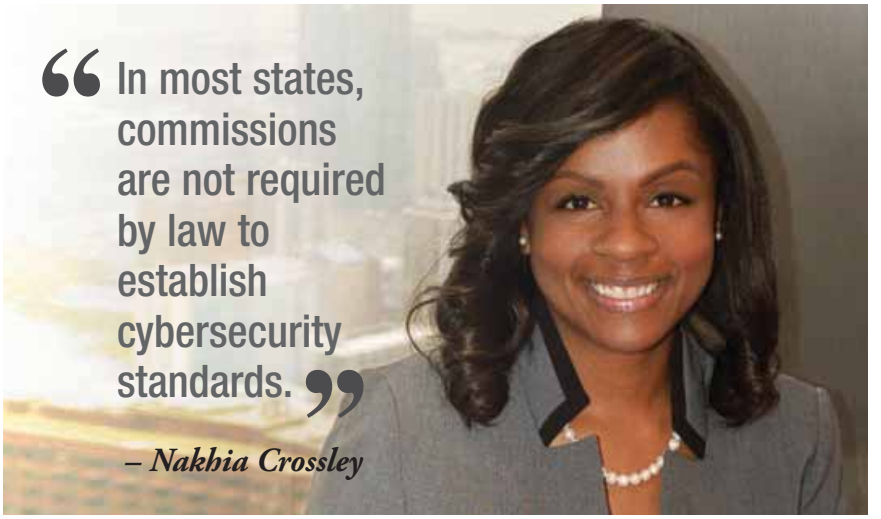
However, where no standards exist, the inquiry becomes challenging, raising the question of how safe is safe enough? Ken Costello of the National Regulatory Research Institute has presented an intriguing yet controversial economic framework in the context of gas pipeline safety that translates well into cybersecurity risk. He argues that the "socially optimal level of safety" is less than perfect. He adds, "As the incremental cost of safety increases, the marginal benefit decreases."

In his white paper, *Balancing Natural Gas Pipeline Safety with Economic Goals*, Costello writes, "Society can have too much safety." Costello points out that commissions must consider numerous objectives, and achieving safety at any cost is not consistent with a balanced approach. He states, "One way to look at costs is that they represent lost opportunities to allocate money

to other activities that might have greater societal benefits."

Costello advocates that under the cost-effectiveness rule, utilities should allocate spending to whatever will produce the greatest safety benefit. A number of gas utilities have vehemently opposed this philosophy in the context of pipeline safety and integrity management program expenditures. But applying it to cybersecurity investments seems reasonable, given the potentially limitless risk and cost associated with protecting the country's infrastructure.

As security and resiliency costs continue to increase, regulators must come to terms with the fact that perfect cybersecurity systems are simply unachievable under contemporary regulatory paradigms. Once regulators accept this notion, they then must work with utilities to assess and manage risk and communicate with the public. They must understand that cyber risk can never be fully managed away.



One issue that has plagued state regulators and electric distribution companies in recent years is cost recovery for spare transformers. It is illustrative of the decisions state regulators are increasingly facing in addressing cyber risks. It is generally well accepted that having spare power transformers readily available is necessary to respond to emergency events. However, regulators have begun to grapple with the appropriate ratemaking treatment, particularly in light of the high cost of transformers.

The Texas PUC recently addressed this issue in a proceeding where Entergy Texas, Inc. sought to recover over seven million dollars for three spare transformers through the company's transmission cost recovery factor. A coalition of Texas cities argued the spare transformers should be excluded because they were not in service, nor were they new transmission construction, and were improperly booked as station equipment.

The Commission concluded that the spare autotransformers did in fact qualify as emergency spares, though it did not approve "of any accounting treatment for transfers of spare autotransformers." It expressly refrained from deciding whether the cost or transfer of spare autotransformers between the Entergy operating companies meets the affiliate transaction standards. The Commission stated it would track all transfers going forward and address the prudency and accounting treatment of affiliate transfers in Entergy's next base-rate case.

Municipal Utilities and Cooperatives

States face another challenge with respect to municipal utilities and electric cooperatives, which are typically subject to little or no PUC oversight, but are often connected to the grid. Municipal utilities and electric cooperatives account for nearly eighty-five percent of the total number of electric companies in the United States and serve more than forty million customers nationwide. For smaller municipal utilities and electric cooperatives with limited resources, investing in cybersecurity may be especially difficult, particularly if they serve lower income rural areas.

To date, some efforts have been made to engage this sector. For instance, the American Public Power Association has conducted outreach, published cybersecurity guidance and offered training on cybersecurity issues. In 2011, the National Rural Electric Cooperative Association also published a guidance document that includes best practices for improving cybersecurity and mitigating the cyber risks associated with the deployment of new smart grid technologies.

However, where only voluntary standards exist, states lack verifiable assurances that municipal utilities and electric cooperatives have sufficiently robust cybersecurity programs in place. Because of their interconnectedness to the grid and to jurisdictional utilities, states must ensure that municipal utilities and electric cooperatives within their borders are taking adequate steps and have sufficient means to ensure the safety and resiliency of their infrastructure.

Another way to effectively bring municipal utilities and electric cooperatives into the fold would be through the creation of a nationwide cybersecurity organization, like that proposed by the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative. The Bipartisan Policy Center reports that the new organization should include the full range of generation, transmission and distribution providers and market operators in the North American power sector, including municipal utilities and electric cooperatives.

Regulatory Lag

The pace at which regulations and legislation develop is no match for the speed and agility of hackers, and the stakes in terms of

(Cont. on page 49)

(Cont. from p. 43)

potential damage can be quite high. Wade Baker, one of the authors of the Verizon 2016 Data Breach Investigations Report, describes the situation quite bluntly: "After analyzing over ten years of data, we realize most organizations cannot keep up with cybercrime, and the bad guys are winning."

U.S. National Security Agency Chief Michael Rogers, agrees, "It's only a matter of when, not if, you are going to see a nation, a group or an individual actor engage in destructive behavior against the critical infrastructure of the United States."

Given these potential harms, it is important that state regulators are kept informed of constantly evolving threats and engaged with the technologies, policies and working groups working to mitigate them. However, the role of the commissioner is very broad and most regulators lack direct experience in cybersecurity.

State regulators must work to foster ongoing dialogues among other regulators, policymakers, law enforcement officials, utilities and additional stakeholders to monitor security and develop programmatic controls capable of countering threats as they evolve.

Information Sharing Concerns

Several legal and logistical barriers can make sharing threat information difficult between the public and private sectors. On the one hand, utilities have a duty to critical infrastructure and business and customer data.

On the other hand, regulators are increasingly requesting or requiring that utilities report on cybersecurity compliance. To balance these objectives, highly secure, confidential channels must exist for utilities and their regulators to openly communicate. Unfortunately, the level of protection afforded to those channels varies widely by state depending on open records laws.

Indiana, for instance, has a comprehensive Access to Public Records Act that provides numerous protections for agency communications, including the discretion to exempt communications "which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack."

This may include a record prepared to prevent, mitigate or respond to an act of terrorism, risk planning documents, critical infrastructure configuration records, security plans and personal identifying information of municipally owned utilities. Given these statutory protections, Indiana utilities have been more willing to engage in meetings and workshops with regulators than utilities in states with less certainty.

Illinois' Freedom of Information Act, on the other hand, presumes that all public body records are "open to inspection or copying." It places the burden of proving that a record is exempt from disclosure on the production of "clear and convincing evidence."

One way to test for cyber readiness is through tabletop exercises.

Illinois exempts disclosure only to the extent that it could "reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public." Consequently, Illinois utilities are discouraged from sharing highly sensitive information with their regulators, given the lack of certainty that such information will be protected.

In states with particularly liberal disclosure laws, new legislation may be necessary to facilitate increased agency-utility collaboration. Ideally, disclosure laws should provide state agencies with discretion as to what information is deemed confidential and impose a lower burden of proof on the agency in the event their designation is challenged.

Where existing state legislation is workable, commissions may also consider directing utilities to report to smaller groups of regulators or staff who possess security clearance. However, the security clearance process can prevent actionable information from getting into the right hands at the right time.

A strong information-sharing regime that helps expedite security clearances and declassify threat information for the public and private sectors helps ensure that cyber threats are shared with entities, helping to mitigate potential threats. PUF

Next month, Part II of this article describes how state regulators across the U.S. are meeting new challenges posed by the need for cybersecurity. The authors outline a handful of best practices that state regulators should consider when evaluating utility cybersecurity programs.

Happy Birthday Alessandro!

Alessandro Giuseppe Antonio Anastasio Volta was a February birthday boy, born on February 18, 1745. In 1799, he invented the battery, proving electricity could be generated chemically. Wow, that was important to mankind.

On top of that, in 1778, he also discovered methane, after reading a paper by Benjamin Franklin on flammable air. So both the electric and gas industries were built on Volta's foundation. The man we honor with the name for our unit of electric potential, the volt, was close with Napoleon Bonaparte. The Emperor made him Count Volta in 1810.