NARUC

Cybersecurity

A Primer for State Utility Regulators

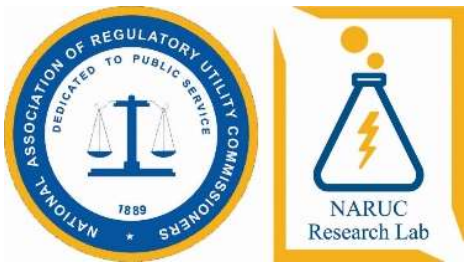
Version 3.0

Miles Keogh
Sharon Thomas

National Association of Regulatory Utility Commissioners

January 2017

With support from the U.S. Department of Energy



Acknowledgments and Disclaimers

This paper was developed by the National Association of Regulatory Utility Commissioners (NARUC) Research Lab. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000818.

State Commission members of NARUC provided the Lab with editorial comments and suggestions. However, the views and opinions expressed herein are strictly those of the authors and may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Please direct questions regarding this report to Miles Keogh, Director of the NARUC Research Lab, mkeogh@naruc.org; (202) 898-2200 and Sharon Thomas, Senior Program Officer, NARUC Research Lab, sthomas@naruc.org; (202)384-1572.

Executive Summary

This primer was prepared by the National Association of Regulatory Utility Commissioners as a tool for policymakers who are charged with making decisions about the electric, gas, water, communications, and transportation systems that are vital to everyday life. Increasingly, these systems are being interconnected with the ability to generate, share, and act on data. With these cyber- capacities come new cyber- vulnerabilities that must be managed by regulators and the infrastructure operators they regulate.

Cybersecurity is unlike many other areas that have historically fallen under the purview of regulators, and the pace of change in this area can be dauntingly fast. However, state utility regulators and others already have many of the tools they need as risk managers to meet these emerging challenges. The primer provides an introductory explanation of the issues, identifies the jurisdictional landscape, and highlights some of the characteristics of good cybersecurity that policymakers should look for. This document also proposes that states engage strategically with cybersecurity to enable and support a thoughtful, risk-based approach that encourages prudent investments by infrastructure operators. The authors make one primary recommendation: that state regulators engage in a process that helps them **become informed** about cybersecurity, **develop a strategy** for engaging on the issue, and **foster dialogue** with industry and other stakeholders to strengthen awareness and improve preparedness. It includes sample questions for states to customize and ask their regulated entities, and highlights other resources that policymakers can turn to as they engage with cybersecurity more deeply.

Introduction

In 2012, we issued our first edition of this primer, noting that reports of cyberattacks were starting to appear in the news. Today, those reports are a daily occurrence, and little question remains that these attacks pose threats to our country's essential utility infrastructure, such as electricity, gas, water, and telecommunications.[1] State utility regulators are asking how to best protect the services, information, and data that are valuable to customers and companies, as well as the country. These regulators are charged with assuring that utility companies provide reliable and affordable service to their customers and putting cybersecurity into the field of view of state regulators. Cybersecurity threats challenge the reliability, resiliency, and safety of the electric grid, and utility spending to address cyber vulnerabilities can impact the bills that customers pay.

This primer addresses cybersecurity—particularly in the context of the electric grid—for state utility regulators, though we know that is it used, and will continue to be useful, to a wide audience of policymakers in this field. The primer provides some conceptual cybersecurity basics for the electric grid and provides links to how regulators can:

- Develop internal cybersecurity expertise;
- Ask good questions of their utilities;
- Engage in partnerships with the public and private sectors to develop and implement cost-effective cybersecurity; and

[1] DHS Critical Infrastructure Sectors are the following: Food and Agriculture; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; Water (http://www.dhs.gov/files/programs/gc_1189168948944.shtm).

- Begin to explore the integrity of their internal cybersecurity practices.

We find ourselves at a critical juncture for infrastructure protection as the grid transitions from a previously isolated environment to a complexly interconnected one. Today's electrical grid interconnects components of our traditional physical electrical infrastructure with less tangible information technology (IT) components such as networks, software, and data. For the purposes of this primer (in which our primary concerns are areas pertinent to state regulators' jurisdiction), when we talk about cybersecurity and infrastructure, we are referring to the cybersecurity of not only the physical distribution and transmission grids, substations, and offices, but also the equipment and systems that communicate, store, and act on data. As these systems grow in intelligence, cybersecurity must encompass not only utility-owned systems, but some aspects of customer and third-party components that interact with the grid, such as advanced meters and devices behind the meter. And more than simply being a function of hardware, cybersecurity is critically important as a function of networks, software, data, and the networks that use data to keep the system operating. Finally, there are human elements to cybersecurity, including system operators, customers, and "bad guys" interacting at all levels of a system. With such a dynamic and broad landscape to consider, cybersecurity cannot be a stagnant prescription handled solely by experts. It should evolve along with the rapid evolution of technology, threats, and vulnerabilities, introducing the building blocks that stand the test of time while still being flexible enough to meet changing cybersecurity requirements.

Why Cybersecurity?

Cyberattacks that cripple the power grid or shut down other infrastructures may be rampant in Hollywood, but it is harder to do in the real world than in the movies. With all the attention given to impossible fictional attacks, it might be helpful to remember that cyberattacks have successfully shut down the grid before.

> *As a worker at the control center was sitting at his desk that day, he watched in perplexity as his computer cursor began moving across the screen on its own, eventually making its way to the buttons that control circuit breakers at one of the region's substations. The cursor seemed to have a mind of its own. The ghost cursor then clicked a box on the screen, which opened the breakers, taking the substation offline. Then a dialogue window opened on the screen asking the user to confirm the action, and the cursor clicked the box to proceed with this action. Astonished by this, the operator desperately tried to regain control of the cursor by moving the mouse away from the breakers on the screen, but he realized his efforts were futile—he no longer had any control over his computer or the control center equipment. The ghost cursor proceeded to move in the direction of another breaker. The operator was then logged out of the control panel, and when he tried to log back in, learned his password had been changed to prevent re-entry. In the meantime, the phantoms in the machine continued opening breakers until nearly 60 substations were offline, leaving 230,000 customers without light or heat. When operators tried to switch to backup power supplies, they were left floundering in the dark at two of the three distribution centers that the attackers had additionally disabled backup power. Their own computers had been completely wiped. Offsite stations were unable to communicate through phone lines because the phone system had been suddenly overwhelmed by a huge number of computer-dialed calls. To restore power, they would have to send workers out to operate distribution systems manually for the foreseeable future until the systems could be completely purged of the attackers.*

This is what it looked like to the system operators at one of the Ukrainian *oblenergos*—distribution utilities—when 230,000 customers lost power in a cyberattack on December 23, 2015. That attack actually began in the spring of 2015 when an email carrying malicious software was opened by one of the IT staff and system administrators who worked for companies that distributed electricity across the Ukraine. This malicious software ("malware") was a virus called BlackEnergy3 that gave network access to hackers. On December 23, 2015, at 3:30 p.m., these attackers used this access to enter the operations systems of the *oblenergos*, and sent commands to disable backup power supply. Next, they overloaded customer call centers with computer-initiated calls so that customers could not report the power outage after the attackers opened breakers. The massive calling strategy bought the attackers more time to execute their plan by creating a longer lag between the substations going offline, and when the operators whose machines were hijacked noticed what was occurring. Additionally, the hackers attacked substation equipment with a first-of-its-kind malware tactic, making those systems inoperable and unable to receive commands. In a *coup de grace*, the aggressors ran attack software that destroyed the operators computer workstations, making them inoperable too, and unable to manage the restoration of power. By around 5 p.m. on December 23, the affected control center posted notes on its website that confirmed it had experienced a power outage, that the cause was a hack, and that restoration would depend on manual operation of its systems. Months later, the *oblenergos* were still deploying operations staff to distribution equipment to operate it manually.

> ***"On the low-impact end of the spectrum are common events, such as copper theft and the types of routine cyber attack common to all business networks in the Information Age. In the intermediate-impact range are events that may involve damage to a single system component in an unsophisticated, unstructured attack. On the high-impact end of the scale are highly-coordinated, well-planned attacks against multiple assets designed to disable the system."***
> **High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," North American Electric Reliability Corporation (NERC), June 2010**

This is a pretty bad scenario, but far from the worst case. A dedicated hacker group, nation-state, or well-funded criminal syndicate could theoretically accomplish worse. The likelier scenario is a smaller attack that compromises data without necessarily affecting the operation of the grid. While the above scenario did occur, the attacks that are easier—and likelier—may be easier to address and mitigate. If regulators (and utilities) can imagine the more drastic possibility, it might be easier to imagine—and prepare for—scenarios of lesser consequence.

Responding to Threats and Vulnerabilities

State governments are already hard at work implementing energy assurance plans across the country that help respond to vulnerabilities, as well as preventing and protecting against threats. There is an important distinction to understand between threats and vulnerabilities. A threat is the potential for an actor, circumstance, or event to adversely affect assets, people, or organizational operations of the system. A vulnerability is a specific weakness at any point in the system that can be exploited by a threat source. A good example is the difference between leaving a door to your house unlocked (creating a vulnerability) and doing so when there are burglars on your street (who pose a threat). Providing true energy assurance in cybersecurity includes addressing vulnerabilities and responding to threats in a way that is timely and assures normal conditions for the near future. The responsibility of prevention, protection, detection, and responding are multi-pronged and shared between industry, local, state, and federal actors.

Given the number of unknown variables that decision-makers need to deal with in cybersecurity, a good way to manage these responsibilities is to support your decisions using risk management— a process that starts with identifying threats, vulnerabilities, and potential consequences, and using. Once identified, decision-makers can use these to prioritize your options for taking action (NARUC wrote extensively about this topic in a separate primer, an introduction to risk management for regulators).[2] We'll revisit this later in the paper.

Where Cybersecurity Fits

Cybersecurity vulnerabilities exist wherever computer systems and data exist. With the advent of smart grid technologies, which layer software on top of utility operations and computer systems, threats become increasingly likely and relevant. Although a smarter grid is generally more reliable, new vulnerabilities appear that must be managed as grids become two-way exchanges of kilowatts, as well as network data, and customer-usage data that may be valuable and desirable to bad actors.[3]

As the electric industry adds more IT systems to the smart grid to improve reliability and efficiency, there are concerns that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and outages.[4]

Threat Sources

Hackers rarely fit a stereotype of a lone actor solely seeking bragging rights. The financial rewards possible from computer theft now vastly outweigh those possible with armed robbery, without the attendant risk to the robber; the integration of intelligence (and cyber vulnerabilities) into critical infrastructure makes utility systems a tempting target for those seeking to undermine national security. As such, criminal syndicates and other organized actors—even nation-states—pose the most significant threats to utility cybersecurity today. Although cybersecurity breaches can be caused by people, they are not always who we think of as "bad guys." Criminal threats to the bulk power system can range from those of minimal impact to those of great consequence. For the purpose of this primer, we will focus on cyberattacks from intentionally malicious actors and how to protect against them, although the steps taken to create cyber secure systems are only one part of an all-hazards approach.[5] Good cybersecurity protects against inadvertent sources—user errors (including accidents), hardware failure, software bugs, operator errors, or plain negligence—as well as intentional attacks. Natural disasters can also play a role: a flooded server room cannot provide service any better than one flooded with data traffic from a denial of service attack. Other resources[6] may be helpful in establishing an all-hazards approach that addresses risks other than intentional cyberattacks.

---

[2] NARUC, *Risk Management in Critical Infrastructure Protection: An Introduction for Utility Regulators*.

[3] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2010: 39.

[4] FERC, "Cyber & Grid Security" (Date retrieved: 12/13/2016): https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

[5] An all-hazards approach takes into account any threat to security, including unintentional or naturally occurring ones, but prioritizes urgent an important risks instead of defending against all hazards equally. A good primer on this concept is online at https://www.ready.gov/planning.

[6] Such as the NARUC/National Association of State Energy Officials (NASEO)/DOE Energy Assurance Guidelines: http://www.naruc.org/Publications/State_Energy_Assurance_Guidelines_Version_3.1.pdf.

Regardless of whether it's a criminal outfit or a nation-state aggressor, the aims and implications of cybersecurity violations vary widely. Gaining system control—the ability to remotely modify and operate the system as a vehicle for attack—is just one of the possible consequences.[7] Data theft (or "exfiltration") is also a known and ongoing problem. The scope of a cyberattack is also an important consideration—size matters. Attacks that affect one person's data or that cripple one meter will generally have less impact than attacks that exploit larger amounts of data, or those that attack not one component, but either multiple components or the network that connects them.

What Are We Protecting? Information Technology vs Operations Technology Attacks

Although natural disasters, human error, software bugs, or equipment breakdowns can be the origins of a system failure, deliberate attacks involve the element of intent—a person at the other end of the operation with the capability to bring down a system specifically outside its existing protective barriers.[8] Malicious attacks threaten utilities on multiple levels in ways that sometimes overlap and compound each other. It may be helpful to visualize the application of cybersecurity in three areas: IT, supervisory control and data acquisition (SCADA) systems, and smart grid. We'll explain each of these components of the data-connected grid and how cybersecurity relates to each.

Information Technology Systems

This is the arena where cybersecurity has historically focused: business process systems such as those found on your laptop computer, as well as in more sophisticated systems and networks that connect data and perform intelligent tasks with that data. It includes both components, like individual workstations, and network components that allow interoperability between components. If IT is all about connectivity—how systems talk to each other—then IT security begins by protecting the network that enables the flow of data through the system, as well as by protecting the data itself. This data can be financial information, a customer's street

Crossing Over from Data Attacks to Physical Impacts: Aurora, Stuxnet, Ukraine

The most common target of cyber attack is sensitive data, but there are examples that highlight the possibility of a successful physical attack that originates in the cyber arena.

In 2006, the Idaho National Laboratory (INL) staged a cyber attack nicknamed "Aurora" that crippled an electric power generator. The attack involved controlled hacking into a replica of a power plant's control system and misusing safety systems to change the operating cycle of the generator, sending it out of control and physically damaging and disabling it.

Emerging in 2009, "Stuxnet" was a self-replicating and –propagating software worm that also had the capacity to physically attack the grid. When an infected USB stick was inserted into a computer, malicious code awakened and surreptitiously dropped a large, partially encrypted file onto the computer, re-writing the programmable logic controller and changing the frequency of spinning drives that it controlled. By 2011, reports were circulating that it had been designed to attack specific centrifuges in Iran; it remains an example of software that can cause physical damage to kinetic systems like those essential to the grid.

Finally, the Ukraine blackouts in December 2015, described at the beginning of the primer, interrupted power for 230,000 customers. It is the signature example of how a cyberattack can interrupt the operation of the power system.

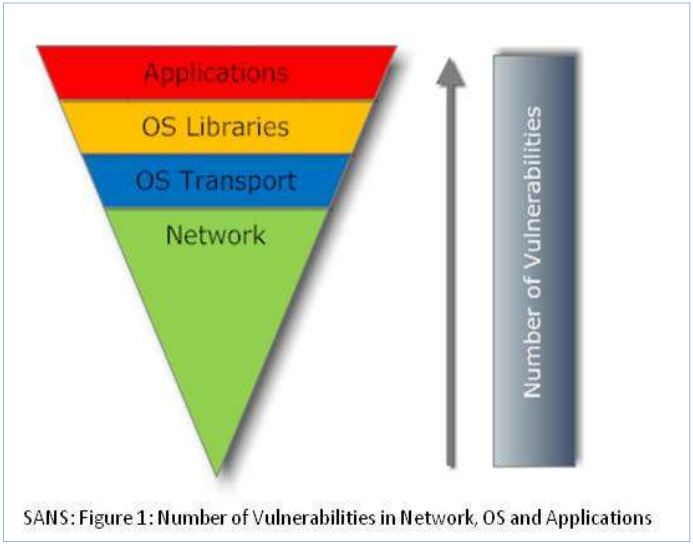
[7] In hacker parlance, the establishment of administrator-level access on a networked system is called "owning" or "pwning" the system. The "p" is pronounced as an "o," which must be – ahem – insiders' humor.

[8] NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 29.

address, phone number, or information about their power usage, to name a few. IT connects all systems, from simple to complex, including communications between systems like the hub or the switch, all the way to the firewall and the server. Considering how valuable the data of utilities' systems are, the communication, transferences, and actions based on this data compound its intelligence value. For IT, cybersecurity not only includes software and hardware strategies—passwords, antivirus systems, firewalls, and logical and physical separation of servers, for example —but also training personnel and creating policies so that their interaction with the IT system enhances, rather than erodes, cybersecurity. Because of this human element, simply upgrading or making hardware more obscure does not equal improved cybersecurity.[9]

Operations Technology (OT) & Control Systems

Although the utility sector has a lot of data worth stealing in the IT arena, one area that distinguishes the cybersecurity measures that utilities take from cybersecurity in other sectors is the degree to which those security concerns are oriented towards control systems like Supervisory Control & Data Acquisition (SCADA) systems. SCADA encompasses systems that monitor and control industrial, infrastructure, or facility-based processes, such as utility operations. They include simple functions such as "on/off," sensor capability, communications capability, and human-machine interface (HMI) that connects them to people operating the system. In other words, they are automatic (and often remote) control devices. SCADA security means the machine does what it is supposed to do and does it accurately. Often the intelligence of the processors on the control systems is limited—certainly it is usually less sophisticated than the capabilities of an IT system like a laptop or server, or even a smartphone. This lack of capability also comes with some simple predictability: with a secure SCADA system, you can trust what your machine is telling you.



SANS: Figure 1: Number of Vulnerabilities in Network, OS and Applications

However, according to executives with SCADA responsibilities, these systems more and more often have connections to Internet Protocol (IP) networks, including the internet in some cases.[10] Even those physically and logically disconnected —"air gapped" —from other systems may be locally or remotely accessible, or have other vulnerabilities to be exploited. SCADA access and control points are also frequently located in remote and unmanned areas of the utility system, and therefore may require either increased physical security or the ability to isolate those points from the overall system if they become compromised.

Security for SCADA systems requires a system-wide understanding of how each of the components fit together so that vulnerabilities can be prioritized and addressed at each point.[11] Depending on the situation, some devices may need to be remotely upgradeable, in which case these devices may need the capability to use encryption, certificates, and authentication. For other devices, this may

[9] Miles Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," *National Association of Regulatory Utility Commissioners*, May 2009: 6.

[10] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 31.

[11] Asset owners should be encouraged to do a risk assessment to determine which vulnerabilities to mitigate. Addressing all vulnerabilities may be cost and performance prohibitive.

be impractical and access might be required to adjust to updated technology. When systems are remotely monitored and maintained, calibration and auditing can be important ways to ensure that they continue giving accurate information and perform functions in a trusted manner. Control systems are not like IT systems, however, in that they often have much longer deployment lifetimes with much rarer software updates and much scarcer physical security measures.

Smart Grid

One problem with securing the smart grid is defining what that is— even experts have a hard time agreeing on what the "smart grid" includes. For this primer, it represents the modernization of electricity infrastructure using information networks. Information networks enable the grid to gather and store data, to create a "dialogue" between all components of the grid, and allow for automatic command and response within the function of the grid. In concept, the smart grid provides so many improvements in situational awareness, prevention, management, and restoration that, in spite of the new vulnerabilities it introduces, it fundamentally makes the electric system more secure and reliable.[12] However, the smart grid enhances the need for cybersecurity because it adds a layer of computer systems and software—all with additional doors to be hacked—to existing utility infrastructure. It may increase the portals through which a cyber threat could enter the system. Keep in mind that the more systems communicate with each other and their human operators, the more channels across which data is shared and, therefore, the more the systems require an assessment of their cybersecurity.

Smart grid technology touches a number of components— from transmission phasor measurement units to smart meters, to home appliances. Therefore, the smart grid requires software to be installed in a way such that if an attack succeeds, components that are compromised components do not threaten the network, and that infiltrators are only able to access data in such a way that the attack is unproductive, undesirable, not valuable, and detectable by operators.[13]

Approaches to Cybersecurity

There are two philosophical approaches to implementing cybersecurity on an intelligent, networked grid: create a checklist of actions to take that address known security problems or prioritize actions based on continually refreshing the answer to the question, "What makes my system more secure?" Both approaches have merits and complement each other.

Using Compliance as a Basis for Cybersecurity

The owners and operators of critical infrastructure have not been sitting idle while cyber threats mount. NERC has developed standards and compliance-based structures that require the operators of the bulk power system to take steps to conform to specific cybersecurity practices. These standards include assessing the systems you have, determining if there are specific vulnerabilities, and then taking action to address these as part of a compliance regime. In practice, these standards appear to be effective for motivating compliance, although some critics note that responding to a compliance regime does not necessarily overlap entirely with responding to a risk-assessed landscape of potential vulnerabilities and threats.

Any regulator interested in cybersecurity will be well-served by becoming familiar with what the NERC Critical Infrastructure Protection (CIP) standards require for the bulk power system. The NERC CIP Standards are enumerated below. On November 22, 2013, FERC approved Version 5 of

[12] Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 6.
[13] *Ibid.*

the CIP cybersecurity standards. Below is a list of NERC's CIP reliability standards for CIP and their enforcement dates. On November 22, 2013, FERC approved the Version 5, which replaces the Version 3 standards. By 2014, NERC began a program to help industry transition directly from CIP Version 3 standards to CIP Version 5.

Number	Title/Summary	Enforcement Date
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	07/01/2016
CIP-003-6	Cyber Security - Security Management Controls	07/01/2016
CIP-004-6	Cyber Security - Personnel & Training	07/01/2016
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	07/01/2016
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	07/01/2016
CIP-007-6	Cyber Security - System Security Management	07/01/2016
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	07/01/2016
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	07/01/2016
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	07/01/2016
CIP-011-2	Cyber Security - Information Protection	07/01/2016
CIP-014-2	Physical Security	10/02/2015

Source: http://www.nerc.net/standardsreports/standardssummary.aspx

The NERC standards have evolved over time, but fundamentally are a requirements-driven approach. Although these standards are robust and a strong improvement over what existed before, state regulators should bear in mind that the NERC CIP Standards are still evolving as they relate to the bulk electric system. Those interested in improving these standards argue that distribution systems and other key areas where cybersecurity remains a concern to state regulators may not be covered entirely by the existing standards. Additionally, those who argue that the CIP standards are incomplete point out that compliance only proves *compliance*; utilities' cybersecurity should be based in *risk assessment*. Risk management includes assessment, mitigation, and continuous improvement, whereas compliance offers a view of cybersecurity at a fixed point in time, not a dynamic picture of it. Utilities may be compliant with the CIP standards and still not be secure. Utilities; utilities may also be secure but not be compliant with the CIP standards. One is not the guarantee of the other. As such, these standards provide an essential floor, whereas using other tools in complement to the standards may yield an even stronger risk-based outcome.

Using Risk as a Basis for Cybersecurity

Understanding risk means understanding the relationship between vulnerability (such as a system with a known but unaddressed weakness), threat (such as a bad actor propagating viruses or

worms), and consequence (such as physical damage and loss of public safety).[14] Simply understanding risks is just the first step: a risk-based approach prioritizes components for protection, as well as the threats and vulnerabilities that require attention. A risk-based approach starts with the assumption that an unauthorized user can and will gain access to data or the system, and thus designs responses based on the value of the data or system that could be compromised by the inevitable access. This calls for prioritizing data and systems based on their value to the organization or other useful criteria such as reliability and privacy. The utility or other organization can then decide which data and systems and programs should have the highest level of cybersecurity, best personnel resources, the right tools, and of course the right budget. Basing a cybersecurity strategy on a risk assessment that identifies and addresses the most significant cybersecurity issues across and within the system will always yield better security results than ineffective "outer wall" approaches to cybersecurity that only focus on denying access to the system. A risk-based approach includes understanding risks, prioritizing them by likelihood, consequence, and potential interactions with other risks, and allocating resources accordingly.[15]

One Risk-oriented Approach for Cyber: The NIST CSF

Organizations responsible for critical infrastructure are increasingly faced with both internal and external threats, which makes the need for having a consistent approach to identifying, assessing, and managing cybersecurity risks even more important. To help address this need, the National Institute of Standards and Technology (NIST) produced a Cybersecurity Framework (CSF), Version 1.0, in 2014 that utilizes a risk-based approach. The CSF was developed in response to President Obama's Executive Order 13636 in 2013, Improving Critical Infrastructure Cybersecurity. It is a voluntary framework that was developed through collaboration between industry and government. The CSF is based on existing standards, and provides guidance to critical infrastructure organizations and others, on how to more effectively manage and mitigate cybersecurity threats. The CSF is a process —not a set of standards or rules—and was designed to be flexible enough that it can be applied to organizations of any size, any cybersecurity risk level, and any level of cybersecurity preparedness, regardless of the industry or country. The CSF provides a common method for organizations to describe their current cybersecurity level; describe their target cybersecurity level; identify and prioritize opportunities for improving (within the context of a continuous and repeatable process); assess progress toward the target state; and communicate among internal and external stakeholders about cybersecurity risk.

The CSF can serve as a foundation for good cybersecurity practices at organizations that don't currently have one in place, or it can enhance an organization's existing practices. The CSF can help organizations develop a better awareness of their cyber risks, as well as how to reduce the risks that they are faced with. It can assist with deciding how to prioritize activities and investments to ensure the delivery of essential services. The CSF organizes the multitude of existing cybersecurity practices, guidelines, and standards (including globally recognized ones), that already exist and have been working well, and provides this information in a more structured, and easier to follow format. An updated version of the CSF, Version 1.1, is anticipated for release later in 2017.

---

[14] U.S. Department of Energy, "Electricity Subsector Cybersecurity Risk Management Process," May 2012.

[15] The authors of this primer at the NARUC Lab also released guidance on how to use and evaluate risk-based approaches in 2016 with "Risk Management in Critical Infrastructure Protection: An Introduction for State Utility Regulators," https://pubs.naruc.org/pub/D10AF40A-AD04-3983-7421-9FBE970D87F3. It's the next paper you should read when you're done with this one.

Cybersecurity Concepts

State regulators are not responsible for building a strong cybersecurity capacity for critical infrastructure—utilities are responsible for this—but it is increasingly important for regulators to recognize underlying concepts of robust cybersecurity when it comes before them in a proceeding. A few of the concepts that should inform a regulator's assessment of a utility's cybersecurity proposal should include:

- Prioritizing systems and networks over components
- Ensuring that human factors are considered
- Deploying defense-in-depth
- Promoting system resilience

Securing Systems and Networks vs. Devices on the Network

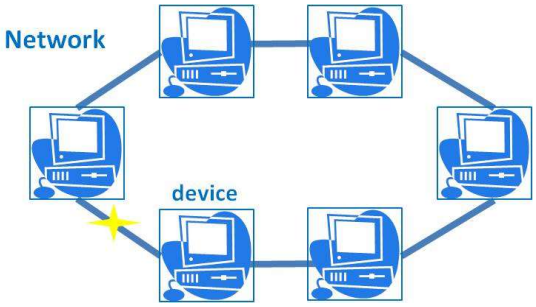


Figure 1 Networks vs. Devices

Cybersecurity may call for securing entire networks, in addition to devices on that network. For example, the meters within a smart grid system can be fortified against attack, but to ensure the entire network of the smart grid system is secure, the components *linking* those meters, as well as every other component in between, must be secured as well. That way, if an attack occurs at one meter, the rest of the system linked to that meter is not also at risk because the components linking them have been protected.[16] This concept was explored in each of the three "flavors" of risk: IT, SCADA, and smart grid.

Personnel Surety: Securing People As Well As Systems

A system is only as secure as the people who run and operate it. Training is essential to ensure that in the event of a cyberattack, personnel are skilled in identifying and responding to the impacts. In case after case, attackers have successfully bypassed even the best security by taking advantage of regular users' naiveté or lack of awareness to give an attacker access. One approach in particular is infuriatingly successful: the "phishing" email with an attachment that has malware. Other approaches—password snatching, brute force cracking, man-in-the-middle keylogging, Structured Query Language (SQL) injection and "pass the hash" attacks—may not need to take advantage of users unwittingly opening the door to their own networks, but phishing has been statistically proven to work often enough that this unsophisticated tactic remains the entryway of choice for even sophisticated hackers. Studies have shown that most clicks occur within hours of receipt, and intrusion detection may take months thereafter. Recruiting end-users as network defenders, through education and strong policies aimed at reducing the success of phishing attacks, may go a long way toward reducing vulnerability.

Personnel can also be "insiders" involved in a deliberate or accidental cybersecurity breach. Identifying key personnel and using background checks is a potential strategy to mitigate this, but once they have been hired, policies that limit an individual's ability to inflict harm may also be

[16] It is worth mentioning that specific cybersecurity mechanisms will likely vary among devices and protection may be stronger or weaker across the devices in the system, depending on their importance and functionality.

important. These policies, such as the Principle of Least Privilege and "Need to Know,"[17] segregate duties. Securing personnel may also include conducting background checks, ensuring expertise through education,[18] offering safe and supportive working conditions, and finally, providing continual training to keep expertise up-to-date.[19] Lastly, effective separation policies for employees, regardless of the reason for separation, should ensure that separated employees' access to facilities, networks, and SCADA systems are terminated as soon as it is appropriate.

Crown Jewels

Not all cyber-connected assets are essential to protect at all cost. Some assets, however, are "crown jewels" – worth protecting at all costs. Other assets may be more like "paperclips" where the expense of protection exceeds the benefit. How do you tell the difference? By reviewing the topology of the network and seeing what is essential, and analyzing its connections to other systems that may serve as an access point for an attack. Conventional wisdom in cybersecurity previously suggested a defense-in-depth approach, requiring many diverse barriers at each layer of potential attack surface. This is a great approach for those with well-developed risk-based resources, but for those just starting, or even those with a well-developed security apparatus, the quickly and ever-changing threats and vulnerabilities would suggest an updated approach. A "crown jewels" approach calls for identifying the ultimate priority assets within the attack surface (these may vary depending on context) and securing these first and most thoroughly. Effective cybersecurity often encompasses physical as well as technological measures – restricted access to server rooms, locks on smart meters, security fencing and cameras at key substations, for example—and these must be incorporated in the above approach. Once the security of the most important resources has been established, working from there towards defense-in-depth may be the right direction. The "crown jewels" approach would suggest protecting the most indispensable people, components, and functions sufficiently first, after which resources should be spent in padding out security towards the overall security of defense-in-depth.

Interdependencies

Although this primer has focused mainly on the electric sectors, attackers will strike any area that seems less-prepared, and cyber threats have been identified to gas, telecommunications, transportation, and other state-regulated utilities. If the industry has and relies on control systems, then it also has vulnerabilities to exploit. In addition to having electrically dependent control systems, regulators must consider the interdependencies of their regulated entities where an electric outage affects gas, telecommunications, and other rate-payer services to an exponential degree on top of the acute effects on the electric grid.

Resilience and Recovery

The electric industry is an incredibly resilient industry. In the event of extreme storms in the past, power lines have been restored much sooner than homes are rebuilt. Resilience of the electric sector to cyberattack should be no less resilient than to a tornado. Whereas defense-in-depth plans for the unexpected, resilience ensures that the unexpected will not persist indefinitely. A resilient system will not only be prepared for deterring, defending against, and mitigating attacks, but also for ensuring quick and efficient restoration through disaster recovery planning in the event that an

[17] Principle of least privilege is defined as having access to the least information or fewest resources necessary to complete a legitimate purpose; "Need to know" is a practice that restricts information or resources in the execution of a task outside of what is critical in order to complete that task, despite clearance level.

[18] A good example is available from the State of Michigan's personnel protocol: www.michigan.gov/cybersecurity.

[19] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 15.

attack compromises the system. Plans should be stored in a way that a cyberattack does not affect access to them, such as installing a backup hard copy in an accessible, but physically secured, location that is water and fireproof.

What Regulators Can Do

The regulatory role in this arena is increasing. More cyberattacks to business processes and NERC CIP Standards compliance are driving new cybersecurity expenditures by utilities that may be featured in future rate cases. The deployment of smart grid adds new cost and reliability elements to this puzzle. Regulators are already hard at work to address cybersecurity risks to the American power grid and the greater infrastructure of utilities. But there's more to be done, and, in the face of shrinking budgets, fluctuating workforce, and the absence of comprehensive legislation, regulators need a dynamic strategy to strike the right balance of security and resources.

As of January 2017, NARUC's Lab has supplied cybersecurity training and technical assistance to 44 states, the District of Columbia, several Canadian provinces, and others. In so doing, we have learned a few things about strong Commission approaches to cybersecurity, which boil down to taking five steps.

It is recommended that State regulators proceed with the following steps:

1. Convene an internal team of staff to set aside time in addition to normal duties to work on cybersecurity to develop essential expertise

2. Develop a strategy that outlines the commission's desired approach, goal, and timeframe for proceeding, and sets expectations for utility performance

3. Ask questions – especially to utilities – and handle answers carefully

4. Engage with companies and other stakeholders in a context that's geared to dealing with cybersecurity as a discrete issue

5. Take action and revisit the strategy and ensuing steps in a cycle of continuous improvement

Step 1: Convene a Cyber Team of Staff
Although regulators will not need to be experts at implementing utility cybersecurity, they will be well-served by asking smart cybersecurity questions of utilities, the entities responsible for conducting risk assessments. These questions are the basis of evaluating prudence, which we will discuss in the next section. Staff members who specialize in cybersecurity at commissions are invaluable resources.

Several states, including Iowa, Washington, Texas, and Pennsylvania have already assembled a cybersecurity team. These states followed a similar approach to forming their teams and executing its mission. This primer suggests that this approach can be tailored to the specifics of your state.

Each state began by articulating the desired role that was most appropriate for its given regulated entities, state-specific assets, and relationship. The teams then generated a strategy that reflected the above articulation before taking action. The starting point and end goal of developing a cybersecurity team were similar in most states, but the steps in between varied – the kinds of skill sets applied, and amount of investment each state made reflected the varying nature of assets, relationships, and regulated entities in those states. One common thread was that top-level leadership commissioned their work and endorsed the outputs, which included tool and resource identification, direct interactions with companies, and the development of questions and draft strategies that the Commission could consider.

Most of these teams helped identify training for staff who interact with the utilities on cybersecurity, and also for staff responsible for implementing cybersecurity of their PUC. It may be valuable to have both types of staff members fluent in the concepts of cybersecurity so that not only those with an information technology workload familiar with cybersecurity, but also those involved with rate cases, siting cases, reliability oversight, and planning will have access to cybersecurity concepts and principles so that this becomes a regular part of the content of a regulatory process when appropriate.

NARUC provides cybersecurity training free of charge through grant-funded programs once or twice per year and convenes cybersecurity expertise at its meetings. It may also be worthwhile to explore what training options may be available through your state's homeland security department, or other in-state sources.

Step 2: Develop a Strategy

Once top-level buy-in is assured and the resources have been allocated to take the work seriously, it's worth developing an internal strategy. As one Commissioner said to me, "Before you go somewhere you should know where you want to go." A strategy can be a public expression of the commission's expectations or an internal expression of the commission's values. The Connecticut Public Utilities Regulatory Authority released a lengthy strategy document; California issued a white paper outlining its regulatory options without making a commitment, and Washington State's strategy started out as a simple paragraph made available to utilities confirming its intention to engage on the issue and setting expectations of proactive partnership by the utilities in the endeavor.

In developing a strategy, you may wish to consider the following questions:

- *What scope do you want your strategy to cover? What sectors? How deep do you want to go?*
- *How does the Commission want to prepare itself? What staffing and resources will be allocated? What training?*
- *Who will be responsible internally? Are new policies needed internally?*
- *What performance requirements do you want from the company?*
- *What reporting/communication do you want, before, during, and after a potential cyber event?*
- *Will your interactions with the utilities and other stakeholders be formal or informal?*
- *Do you want to actively encourage utilities to make cyber investments? Do you want to describe known issues that could constrain investment?*
- *Who else will you work with (law enforcement, information technology, etc.)?*

- *What else do you need to learn to be ready?*

A strategy can get as much or as little attention as you wish to give it. Because authorities, technologies, and attacks change rapidly, it should be revisited as part of continuous improvement, described shortly.

Step 3: Ask Questions
This may be the key role for commissions in cybersecurity. Commissions do not need to become cyber industry authorities or enforcers, but asking a utility a question may motivate the development of a well-founded answer. NARUC has been developing a series of sample questions that originate with some of the interrogatories developed by states with their utilities. These may prove a helpful starting point and are included in *Appendix A* of this primer.

It is very important that questions posed to utilities, however, do not reveal information that could be valuable to a cyberattacker, because answers submitted by utilities during a proceeding are subject to the Freedom of Information Act (FOIA) and can therefore be accessed by the public—potentially including people with malicious intent. Some states have a Critical Infrastructure Confidentiality Statute or other authority that protects against this vulnerability. Please see the Appendix for NARUC's *Sample Cyber Questions to Ask Your Utilities*. It is intended that you will customize these questions to each relevant scenario, while maintaining the phrasing of the questions, which avoids potential cybersecurity risk in the utility's response.

Information Protection
The line between knowing enough to determine that a utility's actions are prudent and knowing so much that the information held by the Commission can pose a cybersecurity risk is a line that commissions should walk carefully. In cybersecurity, the information itself is sometimes the asset worth stealing. To address this issue, states may wish to consider establishing a critical infrastructure information policy. This policy would govern not only the type of information a commission could take possession of (or refuse to take possession of), but also under what circumstances, as well as which access, handling, and storage protocols would govern that data. For example, Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act allows public utilities to restrict certain information from public disclosure and Right-to-Know requests. The Act also puts the onus on state agencies to protect any confidential cybersecurity information belonging to the utility that the state has in its possession, including sensitive parts of emergency or cybersecurity plans.

Commissions should become familiar with their state's information access and transparency laws – such as the FOIA and Sunshine laws—and ensure that sensitive information is not gathered in a context that would enable it to be publicly accessible. Many states have good cybersecurity exemption rules that properly address utility sectors and associated processes while providing automatic protection of information related to cybersecurity. state agencies can develop and communicate their non-disclosure procedures and, where appropriate, may want to consider stronger protections for cybersecurity and information than for commercially sensitive information.

Finally, just because it is legally and procedurally protected does not mean that it's actually cyber secure. Commissions should carefully consider whether they need information before asking for it, because even if they can keep it out of the public record and exclude it from FOIA, it may still be vulnerable to theft via cyberattack.

Just asking questions isn't enough—once the right questions have been asked of utilities, regulators bear the responsibility of understanding the answers to determine whether they represent prudent activities and investments.

Regulators have to determine whether the amount being invested is insufficient or excessive and whether it is allocated appropriately. Regulators must then help prioritize these investments along with all the other proposed spending that a utility proposes in a rate case. Regulators must keep the cost of electricity affordable for customers while asking utilities to spend more on cybersecurity in the face of increasing media attention on stories of cybersecurity threats and vulnerabilities.

Keep in mind that better results will occur when investments are considered with cybersecurity in mind at the front end, rather than adding it to systems as an afterthought. As a result, good cybersecurity is in the DNA of utility investments, not bolted on later. Does the price tag for a meter that uses two-factor authentication single out a line item that articulates its cyber advantages? Does new staff onboarding training that includes anti-phishing awareness cost more than the same training that does not include it? Do governance structures that give cyber risk managers access to company decision-makers show up as cyber expenses, or as standard staffing? What does a "culture of security" look like in a rate case spreadsheet? In other words, financial line items about cybersecurity may be very hard to spot or low cost. Regulators can get a sense of prudent company activity in cybersecurity by framing their questions in the style of a management audit, rather than in the style of a financial audit. Asking about processes, institutional structures, decision-making criteria, and policies may yield greater insights at less risk than asking for a company's "Cyber Plans" outright, or demanding that cyber spending be broken out and evaluated separately.

Step 4: Engage With Your Utilities

Good public process often means openness and broad information disclosure by default, and regulatory activity tends to favor public transparency. This may inadvertently create tension between the transparency of the regulatory process and protection of critical assets. Although regulators are used to maximum disclosure, in a cyberattack, the information itself is the asset worth stealing. As a regulator, if you can engage with the companies on cyber informally, as a discrete issue separated from the baggage of a regulatory proceeding like a rate case, you're likely to get better information. Many states have found they are able to get better contextual information by seeing it at the company's site—this also avoids taking possession of the information and possibly exposing it to public disclosure. That said, some states operate with rules barring these kinds of interactions, and contextual information shared informally at a company's site is difficult to reference as part of an evidentiary record while constructing an order. If it has to be in an open, docketed proceeding, these steps may help:

- Establish a critical infrastructure information handling policy;
- Know your open records laws and rules and implement exemption and protection procedures that properly address utility sectors and associated processes;
- Implement protections for security and cybersecurity info that is stronger than those for commercially sensitive information; and
- Apply all protections to accommodate other parties in a case.

Cyber-secure utility operations is the domain of utilities, and defending against nation-state cyberattacks and cyber terrorism are national defense and law enforcement matters. However, being effectively prepared implicates regulators who oversee and motivate prudent activity by the utilities. Effective cybersecurity takes utility/regulator/security agency partnership and collaboration among these entities.

Step 5: Enact a Cycle of Continuous Improvement
You've developed expertise and a strategy. You've interacted with the companies formally and informally. But the job's not done. Beyond implementing protective measures, any activity informed by risk management means you have to determine the ongoing effectiveness of your risk response measures, monitoring changes and communicating those changes to create a cycle of continuous improvement. Implementation of a Commission cyber strategy is incomplete without structured reporting and feedback. In its excellent 2012 risk management protocol for cybersecurity risk management, the U.S. Department of Energy (DOE) identifies these steps to activate that cycle, working with different levels of an organization so that implementation agents and decision-making authorities mutually update, inform, and reinforce each others' responsibilities in risk management.

The NARUC Resolution Regarding Cybersecurity, adopted on February 17, 2010, calls for "continued vigilance against all potential sources of cyber threat to be both prepared to prevent cyberattacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety and the economy."[20] The resolution encourages regulators to initiate a dialogue with their utilities and their neighboring states. It also supports continually improving the Commissions' engagement, and encourages Commissioners to prioritize the continuous monitoring and evaluating of cybersecurity in collaboration with agencies having expertise in cyber threat management and mitigation in order to remain effective in meeting evolving cyber challenges. Commissioners should regularly revisit their own cybersecurity policies and procedures "to ensure that they are in compliance with applicable standards and best practices."[21]

Regulators from different states have begun to work together to assure improved mutual defense for their utilities. NARUC's Committee on Critical Infrastructure remains an indispensable information hub nationally on cybersecurity for regulators. In the fall of 2016, NARUC Critical Infrastructure (CI) Committee leadership announced a new project to assemble a catalog of information about state PUC activities that pertain to critical infrastructure resilience. The purpose of the CI catalog is to serve as a resource that PUCs can utilize to create awareness about the actions taken by other states to enhance physical and cyber security preparedness, response, and recovery for CI in their states. Participation in the survey is on a voluntary basis. Questions in the survey include topics ranging from general emergency management, cyber emergency management, general cybersecurity, exercises (i.e. tabletops), to information-sharing. The survey was initially sent to thirty-four states that are members of the NARUC CI Committee, and as of January 2017, nineteen states have responded. The remaining sixteen states will be sent the survey early in 2017. This effort represents the first phase of data collection for the catalog, which is intended to be a live document that can be continually updated as PUCs engage in new activities.

Commissions from states in the Mid-Atlantic have had regular meetings on the topic since 2012. New England states jointly hired expertise to conduct risk assessments for their utilities and continue to coordinate closely. Other states have engaged though regional affiliates of NARUC like

[20] NARUC Committee on Critical Infrastructure, "Resolution Regarding Cybersecurity," adopted at the NARUC Winter Meeting of 2010, February 17, 2010.
[21] NARUC Committee on Critical Infrastructure, "Resolution Regarding Cybersecurity," adopted at the NARUC Winter Meeting of 2010, February 17, 2010.

the MidAmerica Association of Regulatory Commissions (MARC) and the Southeastern Association of Regulatory Utility Commissions (SEARUC).

Conclusion

Absolute cybersecurity is neither attainable, nor is it the end goal. What's more, according to NERC, addressing high-impact, low-frequency risk like cybersecurity requires the re-allocation of "already strained human and financial resources available to the sector."[22] Therefore, cybersecurity is best approached through a nimble and complex balance of functionality, security, and cost. The reality of a "perfect" defense against cyberattacks has a cost that may, and often does, outweigh the value of the information it protects. Simply put, the energy sector cannot expect to "gold plate" the grid. Planning for, protecting against, detecting, and responding to cyberattacks must take into account a dynamic relationship of systems, physical components, people, and their function.

State utility regulators can and should:

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

Regulators are already doing significant work to protect the grid, but the key to successful cybersecurity may prove to be the development of a partnership between public and private actors to create a cybersecurity structure and culture that can meet current needs while also being flexible enough to meet a quickly evolving threat.

[22] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," pg. 23

Appendix A: Sample Cyber Questions to Modify and Ask Your Utilities

The following questions grew out of several PUCs efforts to ask critical cybersecurity questions of utilities in an effort to ensure reliable electricity for their rate payers. NARUC has built the following list from those original questions, editing where necessary for sensitivities, clarity, and general usage so that these questions could be used in commissions across the country. These are general questions, they are not exhaustive, nor are they all appropriate for every scenario or region. You must adapt the questions to your own taste, but when you do so, make sure the answers will not create vulnerabilities. These questions not only generate answers from utilities, but also inspire their action to meet any gaps in current operations. Your utilities may not be particularly forthcoming with some of their answers, but their answers create a dialogue of understanding and responsibility in the event of a cyberattack.

Your needs for your PUC will vary —please modify these questions before using them in order to suit your needs. For example, drop the questions that are too difficult or are unnecessary! You do not need to use questions below which you think will yield answers that contain unnecessary or overly complex information. Where questions below reference a process or a plan that the utility probably has in hard copy, you may want to ask to see a copy of it.

You may want to describe to the utility how you will handle and safeguard the responses to these questions. Lastly, and most importantly, *do not ask questions whose answers can create vulnerabilities*.

Planning

Having a plan indicates that the response isn't piece-meal, reactive, or fragmented. Asking planning questions aims to encourage proactive and strategic action on the part of the utilities, rather than a patchwork response.

1. Does your company have a cybersecurity policy, strategy, or governing document?
2. Is the cybersecurity policy reviewed or audited? Internally or by an outside party? What qualifications does the company consider relevant to this type of review?
3. Does your cybersecurity plan contain both cyber *and* physical security components, or does your physical security plan identify critical cyber assets? (See the *Glossary, Appendix 2*, for helpful definitions).
4. Does your cybersecurity plan include recognition of critical facilities and/or cyber assets that are dependent upon IT or automated processing?
5. Are interdependent service providers (for example, fuel suppliers, telecommunications providers, meter data processors) included in risk assessments?
6. Does your cybersecurity plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?

7. Has your organization conducted a cyber risk or vulnerability assessment of its information systems, control systems, and other networked systems?

8. Has your company conducted a cybersecurity evaluation of key assets in concert with the National Cyber Security Division of the U.S. Department of Homeland Security (DHS)? Has your company had contact with the National Cyber Security Division of DHS or other elements of DHS that may be helpful in this arena?

9. Has your cybersecurity plan been reviewed in the last year and updated as needed?

10. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?

11. What is your process/plan for managing risk? (Example: DOE/NIST/NERC Risk RMP)

12. Has your company undergone a whole-system, comprehensive cybersecurity audit or assessment? When and by whom?

Standards

Standards are an important driver of enforceable action with which regulators can attempt to ensure utilities' compliance.

13. Is the company currently in compliance with NERC CIP-002 through CIP-014?

14. Does the company use the NIST Cybersecurity framework?

15. Does the company leverage resources like the ESC2M2 or DOE Risk Management Process for cybersecurity?

16. What collaborative organizations or efforts has your company interacted with or become involved with to improve its cybersecurity posture (such as NESCO, NESCOR, Fusion centers, Infragard, US-CERT, ICS-CERT, E-ISAC, SANS, HSIN, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.)?

17. Can your company identify any other mandatory cybersecurity standards that apply to its systems? What is your company's plan for certifying its compliance or identifying that it has a timetable for compliance? *(Note: PUCs might also need to first establish standards for compliance they find suitable.)*

18. Are there beyond-compliance activities? Absent cybersecurity standards specified by state regulatory authorities in regard to the distribution portion of the electrical grid, what are you doing to get in front of this?

19. How do you determine which systems, components and functions get priority in regard to implementation of new cybersecurity measures?

20. Is cybersecurity addressed differently for each major electrical component: distribution, transmission, generation, retail customers?

Reporting

Not all attacks rise to the level of reporting to authorities. These questions explore the topic but are focused on helping the Commission understand the status quo, in case additional reporting structures would be beneficial.

21. How do you report cyberattacks? What is the threshold for notifying law enforcement?
22. Are you currently required to report any cyber incidents to any federal or state agencies?
23. Do you report cyberattacks or breaches to the PUC? What is the threshold for doing so?
24. Have you articulated reporting elements for the kinds of information you disclose in the event of an attack?
25. Do you currently report cyber incidents to the NCCIC?
26. Are you currently required to report any cyber incidents to any federal or state agencies?

Partnerships

Alliances across public and private sectors are essential for information-sharing, planning, and situational awareness around cybersecurity for critical infrastructure. Regulators can use these questions to learn about their regulated utilities' information-sharing practices. Additionally, regulators can use these questions to gain an understanding of the nature of utilities' relationships with key organizations at the local, state, regional, and federal levels.

27. Do you participate in a briefing process with other decision-makers (such as PUCs in neighboring states or other regions, governors, federal partnerships, etc.)?
28. Would the company be willing to provide a presentation to staff (as a closed, *in-camera* and non-disclosable setting with no documentation or materials coming into possession of the PUC)?
29. Discuss what the PUC can do to assist your company in the area of cybersecurity.
30. Identify whether the company has identified points of contact for cybersecurity:
    a. Emergency management/law enforcement?
    b. National security? DHS, including protective and cybersecurity advisors?
    c. Fellow utilities, ISO/RTO, NERC CIPC, others?
    d. NESCO, VirtualUSA, Einstein, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC?
    e. Interdependent system service providers?

Procurement Practices

Although the information of procurement seen upstream to vendors may only be proprietary to the utility, the decisions the vendor makes around procurement may contain key elements for cybersecurity. The questions below cover these aspects of procurement.

31. Has your organization conducted an evaluation of the cybersecurity risks for major systems at each stage of the system deployment lifecycle? What has been done with the results?

32. Are cybersecurity criteria used for vendor and device selection?

33. Have vendors documented and independently verified their cybersecurity controls? Who is the verifier and how are they qualified?

34. Are there third-party providers of services whose cybersecurity controls are beyond the ability of your organization to monitor, understand, or assure? Has your organization explored whether these may create cybersecurity vulnerabilities to your operations?

35. Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity, and website hosting?

36. Has the company managed cybersecurity in the replacement and upgrade cycle of its networked equipment? Does this include smart meters?

37. What kind of guidance do you follow to ensure that your procurement language is both specific and comprehensive enough to result in acquiring secure components and systems? (Note: Does your company include Cyber Security Procurement Language for Control Systems within its Procurement Language? Available at http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf IEC 62443.)

Personnel and Policies

Personnel, the people who run the systems we aim to protect, are key to ensuring cybersecurity. The way employees are hired, trained, and separated from operations can make or break cybersecurity.

38. Does your organization have a company-wide policy regarding best practices for cyber?

39. Does your company provide end-user training to all employees on cybersecurity, either as part of general staff training or specifically on the topic of computer security and company policy?

40. Does your company provide resources to improve end-user awareness of phishing, malware, indicators of compromise, and procedures in the event of a potential breach?

41. Is there a cybersecurity budget? What is the current budget for cybersecurity activities relative to the overall security spending?

42. Are individuals specifically assigned cybersecurity responsibility? Do you have a Chief Security Officer and does that person have explicit cybersecurity responsibilities?

43. Does your company use IT personnel directly, use outsourcing, or use both approaches to address IT issues? For companies that lack a full IT department, explain if one individual in your company is held responsible for IT security. (You may want to ask the same questions in regard to Operations Technology (OT) (i.e., energy operations) security; larger companies may have separate staffs.)

44. What training is provided to personnel that are involved with cybersecurity control, implementation, and policies?

45. What personnel surety/background checking is performed for those with access to key cyber components? Are vendors and other third parties that have access to key cyber systems screened?

46. For the most critical systems, are multiple operators required to implement changes that risk consequential events? Is a Change Management process in place, especially in regard to systems that could present a risk to electrical reliability?

47. Has business process cybersecurity has been included in continuity of operations plans for areas such as customer data, billing, etc.?

48. Describe the company's current practices that are used to protect proprietary information and customer privacy and personal information. Does the company have an information classification and handling policy?

49. Does the company collect personally identifiable information electronically? What type of information (name, address, social security number, etc.) is collected? Is there a policy for the protection of this information? How is your company ensuring that any third parties you deal with are also keeping this information secure?

Using risk management for cybersecurity

50. Is there a person at your organization who assesses vulnerabilities, consequences, and threats?

51. How do you prioritize risks? With all the changes in the grid, how often do you update your priority list?

52. What criteria do you use to prioritize risks? What process do you go through? Which personnel are involved with this?

53. How do you assess vulnerabilities to your system and assets? (e.g. getting alerts from ICS-CERT; regularly applying patching programs; or with vulnerability scanning software)?

54. Do you have an internal or external company performing your vulnerability assessment? (e.g. a third party conducts these assessments)?

55. How do you assess threats to your system and assets? What are your information sources? (e.g., (ICS-CERT; IT/OT vendors; or communication channels such as ISACs)?

56. Do you use contingency-driven consequence analysis?

57. Do you have a process for looking at consequences of cyber incidents that informs your risk management process?

Implementation

58. How do you determine the effectiveness of your strategies?

59. Do you report on this effectiveness of strategies? Who do you report to? How often?

60. What needs to happen for improvement actions to take place? (What are hindrances and what can be done to overcome them?) What decision-making structures can authorize cybersecurity improvements?

61. How do you decide which activities to take action on regarding a detected cybersecurity threat? (such as by looking at case studies or deciding which activities to take action on based on conversations with other utilities about how they handled it)

62. How can you tell if the actions you plan to take will contain the impact of a potential cyber threat?

Response & Recovery

63. Is there a person at your organization who coordinates responding to threats and recovering from them?

64. Do you consider legacy alternatives (analog systems, manual mode, or "conservative operations") to provide redundancy to systems with cyber vulnerabilities?

65. Do you have a consumer communication plan or a way of dealing with customer perceptions and expectations?

66. Do you participate in sharing communication, analysis, and mitigation measures with other companies as part of a mutual network of defense?

67. Are response processes and procedures executable and are they being maintained?

68. Is the information shared consistent with the response plan? Is coordination with stakeholders consistent with the response plan?

69. Do your response plans include lessons learned and mechanisms for continual improvement?

70. Are your recovery strategies regularly updated?
71. Do your recovery plans incorporate lessons learned?
72. Do you have a plan in place for reputation management after an event?
73. Are recovery activities communicated to internal stakeholders and executive and management teams?

Process Questions

74. Are indicators of compromise shared with employee end-users and leadership?
75. Does your company communicate to employees the process for reporting and containing compromise?
76. Do you have a baseline configuration of IT/ICS that is used and regularly maintained?
77. Do you have a System Development Life Cycle plan that is implemented to manage systems?
78. Do you keep key information backed up, maintained, and tested periodically? Does your organization have a policy for storing hard copies of relevant essential documents for continuity of operations purposes?
79. Do you have policies and regulations in place regarding the physical and operating environment for organizational assets?
80. Does your organization destroy data according to policies in place?
81. Are protection processes being continuously improved?
82. Is maintenance and repair of organizational assets performed and logged in a timely manner, with approved and controlled tools?
83. Is remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?
84. Are audit/log records determined, documented, implemented, and reviewed in accordance with your organization's policies?
85. Is removable media protected and its use restricted according to your organization's policies?
86. Is access to systems and assets controlled, incorporating the principle of least functionality?
87. Are communications and control networks jointly or separately protected?

Governance Questions

Top-level leadership creates organizational cultures. Having a "culture of security" is central to assuring cybersecurity in an environment where many employees have the capacity to provide—or prevent—access to attackers. These questions explore the connection between cybersecurity and decision-making priorities at the top of the organization.

88. Are cybersecurity responsibilities assigned? Is this done separately from information technology responsibilities?

89. Is there a method of coordinating these responsibilities?

90. Is an organizational information security policy established?

91. Are information security roles and responsibilities coordinated and aligned with internal roles and external partners?

92. Does senior leadership have access to cybersecurity risk information?

93. Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?

94. Do governance and risk management processes address cybersecurity risks?

95. Do you have an enterprise-wide risk management program that includes cybersecurity?

96. Have you had outside experts look at your cybersecurity plans? (such as law enforcement or a federal agency)

97. How do you monitor your cybersecurity posture on business IT systems and ICS systems and communicate status and needs to leadership?

Systems and Operations

Be aware that as the questioning agency, you want to consider carefully whether answers to the below questions are needed and, if so, whether the answers to them could create vulnerabilities to the system. Modify them to your needs accordingly.

98. Is cybersecurity integrated between business systems and control systems? For the existing grid and for the smart grid?

99. Have logical and physical connections to key systems been evaluated and addressed?

100. Does the company maintain standards and expectations for downtime during the upgrade and replacement cycle?

101. Does the company have equipment dependent on remote upgrades to firmware or software, or have plans to implement such systems? Does the company have a plan in place to maintain system cybersecurity during statistically probable upgrade failures? Is

there a schedule for required password updates from default vendor or manufacturer passwords?

102. Has cybersecurity been identified in the physical security plans for the assets, reflecting planning for a blended cyber/physical attack?

103. What network protocols (IP, proprietary, etc.) are used in remote communications? Is the potential vulnerability of each protocol considered in deployment?

104. Does the company have a log monitoring capability with analytics and alerting—also known as "continuous monitoring"?

105. Are records kept of cybersecurity access to key systems?

106. Are systems audited to detect cybersecurity intrusions?

107. Are records kept of successful cybersecurity intrusions?

108. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?

Appendix B: Cybersecurity Glossary

Glossary	
All-Hazards Approach	Comprehensive approach to security that includes intentional, unintentional, man-made, and naturally occurring threats to the electric grid
Attestation[23]	The validation of all aspects of a component that relate to its safe, secure, and correct operation
Authentication[24]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources
Authorization[25]	Verifying a user's permissions (after the user had been authenticated) for accessing certain resources or functionality
Bandwidth[26]	The amount of information that can be passed through a communication channel in a given amount of time, usually expressed in bits per second
Bitcoin[27]	A new form of digital currency created in 2009 that can be used to buy merchandise anonymously. Bitcoins are not tied to any country or subject to regulation, so international transactions have been made cheaper and easier. Transactions take place without a middle-man, so banks are not involved. Additionally, there are no transaction fees and no need to give your real name. Bitcoin is becoming more accepted by merchants.
Boundary protection[28]	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Bulk Electric System (BES) Cyber Asset[29]	A cyber asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact facilities, systems, or equipment, which, if

[23] Evgeny Lebanidze and Craig Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," *National Rural Electric Cooperative Association Cooperative Research Network* (2011): 113.
[24] *Ibid.*
[25] *Ibid.*
[26] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=5692.
[27] CNN Money, Date retrieved: 12/20/2016, http://money.cnn.com/infographic/technology/what-is-bitcoin/
[28] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[29] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012: 9.

	destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system.
Connectivity[30]	The minimum number of nodes or links whose removal results in losing all paths that can be used to transfer information from a source to a sink.
Confidentiality[31]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Contingency[32]	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element.
Control Center[33]	Facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations.
Credential[34]	Information passed from one entity to another to establish the sender's access rights or to establish the claimed identity of a security subjective relative to a given security domain.
Critical Assets[35]	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.
Critical Infrastructure[36]	The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

[30] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6637.
[31] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[32] *Ibid*.
[33] NERC, "Glossary of Terms Used in NERC Reliability Standards," 13.
[34] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6764.
[35] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[36] U.S. Department of Homeland Security, "Critical Infrastructure" (May 23, 2012): http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

Cyber Asset[37]	Programmable electronic devices, including the hardware, software, and data in those devices.
Cybersecurity Incident[38]	A malicious act or suspicious event that: 1) compromises, or was an attempt to compromise, the ESP or PSP, or 2) disrupts, or was an attempt to disrupt, the operation of a BES cyber system.
Denial of Service (DoS) [39]	Unauthorized prevention or (for time-critical operations) delay of any part of an information system (IS) from legitimate access or functioning.
Deterrence	Designing a system to that an attack would be unprofitable, limited in scope and easily traceable.
Electronic Security Perimeter (ESP)[40]	The logical border surrounding a network to which systems are connected.
Energy Assurance	Infrastructure that is robust, secure, provides reliable energy, and is able to restore services rapidly in the event of any disaster.
Encryption (also encipherment)[41]	The cryptographic transformation of data that produces coded text.
Firewall[42]	A network security device that monitors incoming and outgoing network traffic and helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. A firewall can be hardware, software, or both.
Firmware	Embedded software that cannot be modified, but allows reading and executing software.
Header[43]	The portion of a message that contains information used to guide the message to the correct destination. *Note:* Examples of items that may be in a header are the addresses of the sender and receiver, precedence level, routing instructions, and synchronizing bits.
Identity-Based Access Control[44]	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

[37] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[38] NERC, "Glossary of Terms Used in NERC Reliability Standards," 14.
[39] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[40] NERC, "Glossary of Terms Used in NERC Reliability Standards," 18.
[41] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=8119.
[42] Cisco, Date Retrieved: 12/20/2016, http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
[43] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=4731.
[44] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

Impact[45]	Damage to an organization's mission and goals due to the loss of confidentiality, integrity, or availability of system information or operations.
Incident[46]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information Security[47]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Information System[48]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (*Note*: information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.)
Information Technology (IT)	A discrete set of electronic information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or dispositioning information.
Integrity[49]	Guarding against improper information modification or destruction; includes ensuring the non-repudiation and authenticity of information.
Internet Protocol	A formal set of conventions (both semantic and syntactic) governing the format and control of interaction among parts of the system that communicate with each other.
Interoperability[50]	Ability of diverse systems and their components to work together; enables integration, effective cooperation and two-way communication among the many interconnected elements of the electric power grid

[45] *Ibid.*
[46] *Ibid.*
[47] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[48] *Ibid.*
[49] *Ibid.*
[50] NIST, "NIST & the Smart Grid," (May 23, 2012): http://www.nist.gov/smartgrid/nistandsmartgrid.cfm.

Least Privilege	Principle of having access to the least information or fewest resources necessary to complete a legitimate purpose
Latency[51]	Refers to the speed with which network data is transmitted or processed. A system with low latency communicates more quickly, while a high latency connection generally communicates less frequently and has longer delays
Loss Containment	Protecting the overall system, even if some individual components can be compromised
Malware[52]	A malicious software program that can infect your computer or other electronic devices, causing harm. Examples of malware are viruses, worms, Trojans, and spyware.
Management Controls[53]	The security controls (i.e., safeguards or countermeasures) of an information system that focus on the management of risk and of information system security
Need to know	A practice that restricts information or resources in the execution of a task outside of what is critical to complete that task despite clearance level
Network (computer network)[54]	A collection of hardware components and computers interconnected by communication channels that allow for the sharing of resources and information
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message
Operational Controls	The security controls (i.e., safeguards or countermeasures) of an information system that are primarily implemented and executed by people (as opposed to systems)
Packet[55]	The sequence of binary digits transmitted and switched as a composite whole

[51] Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 5.
[52] Kaspersky Lab, Date retrieved: 12/20/2016, http://usa.kaspersky.com/internet-security-center/internet-safety/what-is-malware-and-how-to-protect-against-it#.WFlmAvkrKUk.
[53] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[54] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6555
[55] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=30770

Phishing[56]	A spoof that tricks people into divulging sensitive information such as usernames, passwords, or credit card numbers. Phishing can be carried out by email, over the phone, or with a website. The motives are generally to steal money or a user's identity.
Physical Security Perimeter (PSP) [57]	The physical border surrounding locations in which cyber assets, systems, or electronic access control systems reside and for which access is controlled
Potential impact[58]	The loss of confidentiality, integrity or availability that might be expected to have: 1) a limited adverse effect (FIPS 199 low); 2) a serious adverse effect (FIPS 199 moderate); or 3) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals
Privileged User[59]	A user that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform
Programmable Logic Controller (PLC)[60]	A digital computer used for the automation of electromechanical processes

[56] Norton, Date retrieved: 12/20/2016, https://us.norton.com/cybercrime-phishing

[57] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012:36.
[58] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[59] *Ibid.*
[60] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.

Ransomware[61]	A malicious form of software that locks your computer or files and requires you to pay money to get the decryption code to unlock your files or device.
Resilience[62]	Robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event.
Right-to-Know	Legal principle that a citizen has the right to know a piece of information about a potential hazard.
Risk[63]	Measure of the extent to which an entity is threatened, typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Security risks related to information security arise from the loss of confidentiality, integrity, or availability of information or information systems with potential adverse impacts on operations.
Risk Management	The process of conducting a risk assessment, implementing a risk mitigation strategy, and employing of techniques and procedures for the continuous monitoring of the security state of the information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place – synonymous with risk analysis.
Risk severity[64]	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization's mission and goals if it does occur
Role-based access control[65]	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals

[61] Microsoft Malware Protection Center, Date retrieved: 12/20/2016, https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D

[62] NARUC, "Resilience in Regulated Utilities," November 2013, https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D.

[63] *Ibid.*

[64] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.

[65] *Ibid.*

Sensitive information[66]	Information of which the loss, misuse, unauthorized access or modification could adversely affect the organization, its employees or its customers
Smart Grid	Modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a "dialogue" between all components of the grid, and allowing for automatic command and response within the function of the grid
Social Engineering[67]	This refers to psychological manipulation of people into divulging sensitive information or performing certain actions.
Supervisory Control and Data Acquisition (SCADA)	Systems that monitor and control industrial, infrastructure, or facility-based processes, such as automatic (and often remote) control devices. They include simple functions such as "on/off" and sensor capability, communications capability, and the human-machine interface (HMI) that connects them to people operating the system
Supply Chain[68]	A network between a company and its suppliers, to produce and distribute a product. The supply chain refers to the organizations, people, and other resources involved in getting the product or service from the supplier(s) to the customer.
Threat	The potential for an actor, circumstance, or event to adversely affect assets, people, or organizational operations of the system
Traffic[69]	The information moved over a communication channel, including the quantitative measurement of the total messages and their length, expressed in CCS or other units, during a specified period.
Virus	An unwanted computer program that replicates itself and spread from one computer to another. "Virus" is often used incorrectly to refer to malware, including adware and spyware programs, which do not have a reproductive ability.
Vulnerability	A specific weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Appendix C: Essential Resources for Regulators

[66] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 116.
[67] Symantec, "What is Social Engineering?," 03/16/2015, https://www.symantec.com/connect/blogs/what-social-engineering.
[68] Investopedia, Date retrieved: 12/20/2016, http://www.investopedia.com/terms/s/supplychain.asp.
[69] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=649

Cybersecurity remains an area where a lot of work needs to be done, but it is worth noting that many institutions and frameworks have been set up that have already made an enormous amount of progress. Some of these are listed below. Many of these groups are open to state personnel to monitor, join, and participate in, and this may be an important way to become appropriately engaged with companies and other stakeholders working on these issues before they emerge in the context of a hearing room. Particularly if a state has multiple regulated utilities, information sharing among utilities and potentially PUCs may be a very important step toward coordinated cyber defense.

Drivers for Cybersecurity Expenditures

Aside from good business practices by the utilities that dictate that they should prevent attacks on their systems, state regulators should understand three key additional areas that motivate and inform smart utility investments in cybersecurity: laws, enforceable standards, and voluntary best-practice guidance.

Industry standards enforce legislation that utilities must meet, and these standards do not come cheaply. Standards require additional resources in the form of employees, hours, and technology, all of which increases the cost of providing reliable electricity to the customer. Therefore, the standards of cybersecurity that protect the customer are then ultimately paid by the customer. So what are these standards and who sets them? Some of the most important sets of standards are described in this section.

NERC CIP

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

The first step for developing cyber expertise is to understand, and where possible engage with, the NERC CIP Standards. These standards are the impetus behind many cybersecurity investments. NERC CIP Standards are mandatory for utilities to comply with and provide a baseline set of security measures to protect the bulk power system. NERC's CIP efforts include standards development, compliance enforcement, and supporting and providing technical subject matter expertise to the program. The committee consists of industry experts and reports to NERC's board of trustees in the areas of cybersecurity, physical, and operational security. DOE designated NERC as Electricity Sector Coordinator for critical infrastructure protection, which entails liaising with government agencies.

NIST Cybersecurity Framework(CSF), Version 1.0

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Through collaboration between government and the private sector, the National Institute of Standards and Technology (NIST) created a voluntary, risk-based cybersecurity framework that was released in 2014. This Framework consists of industry standards and best practices to help organizations reduce and better manage their cybersecurity risks. It uses common language to address and manage cybersecurity risk in a cost-effective way, without placing additional regulatory requirements on businesses. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. An updated version of the Framework, Version 1.1, is expected to be released later in 2017.

NIST National Cybersecurity Center of Excellence

https://nccoe.nist.gov/

Established three years ago by NIST, the National Cybersecurity Center of Excellence is a public-private collaboration that works to accelerate the development and use of secure, standards-based technology for companies. The Center has partnered with 22 market-leading IT companies that contribute hardware, software, and expertise. The Center asks industry members about their cybersecurity issues and then forms a team of experts from cybersecurity technology companies, federal agencies, and academia to address each problem. For each example solution, the Center publishes a publicly available guide with materials and information to help deploy the example solution.

NIST Smart Grid Interoperability Panel and the Smart Grid Cybersecurity Committee
http://www.sgip.org/
The NIST Smart Grid Interoperability Panel (SGIP) is comprised of a range of stakeholders and working groups that work together to drive the development and adoption of standards for interoperability for electric distribution systems. SGIP additionally serves as a voice for the Internet of Things in the energy sector, and also convenes multi-stakeholder workgroups to address distributed generation activities. One of the key workgroups of SGIP is the Smart Grid Cybersecurity Committee (SGCC). SGCC currently works closely with NIST, DOE, and various electrical utilities in the United States and Canada.

Topics that the SGCC are involved with include: providing recommended security requirements that may be used by strategists, designers, implementers, and operators of the grid; creating and maintaining a logical reference model of the Grid, which enables the creation and maintenance of a logical security architecture; identifying privacy risks with developed or emerging interoperability standards for the grid, and then determining the most appropriate practices for mitigating the risks; identifying cybersecurity-specific gaps and challenges; assessing proposed standards and requirements for adoption into the SGIP Catalog of Standards; and developing cybersecurity and privacy resources that can benefit stakeholders. The SGCC developed the NIST Interagency report (NISTIR) 7628, Guidelines for Smart Grid Cybersecurity, available here: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

The NARUC/NASEO Energy Assurance Guidelines
The National Association of State Energy Officials (NASEO) runs an energy assurance program to address state-level coordination on critical infrastructure protection. Other national organizations along the lines of NARUC and NASEO are doing their part to address cybersecurity needs for the energy sector and to serve as resources to government decision makers. You can learn more about NASEO's Energy Assurance Program here: http://naseo.org/energyassurance/.

Securities and Exchange Commission Corporation Finance Disclosure Guidance: Cybersecurity
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
In October 2011, the SEC released this guidance to clarify the cybersecurity responsibility of publicly traded companies. The guidance is intended to assist companies with preparing disclosure obligations relating to cybersecurity risks and cyber incidents. Federal securities law requires that publicly traded companies report "material" risk – something that was not clearly defined or followed for cybersecurity risks before this document was released.[70] This is a vital moment because now a publicly traded company can consider cybersecurity as a business investment.

[70] Jay Rockefeller and Michael Chertoff, "A new line of defense in cybersecurity, with help from the SEC," *The Washington Post*, November 17, 2011, http://www.washingtonpost.com/opinions/a-new-line-of-defense-in-cybersecurity-with-help-from-the-sec/2011/11/15/gIQAjBX8VN_story.html.

DHS Cross Sector Working Group – CIPAC
http://www.dhs.gov/files/committees/gc_1277402017258.shtm
The DHS Cross-Sector Security Working Groups include the Critical Infrastructure Partnership Advisory Council (CIPAC), which facilitates coordination between governmental entities and critical infrastructure owners and operators. It also operates a forum in which government and critical infrastructure key resource owners can coordinate resilience and critical infrastructure protection measures.

NCCIC Overview
https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
The National Cybersecurity and Communications Integration Center (NCCIC) falls under the DHS Office of Cybersecurity and Communications as the central location for coordinating and integrating operations of cybersecurity and communications reliance. The NCCIC is a 24/7 cyber situational awareness, incident response and management center. It also shares information between public and private partners regarding vulnerabilities, incidents, and mitigation measures. Subscriptions, news feeds and other updates are also available at no cost at the bottom of this page: https://www.us-cert.gov/nccic.

DHS Cyber Security Evaluation Tool
https://ics-cert.us-cert.gov/Assessments
The Cyber Security Evaluation Tool (CSET) was created by DHS to support organizations in protecting their key national cyber assets. Cybersecurity experts, under the direction of the DHS National Cyber Security Division (NCSD) and with assistance from NIST developed this tool to provide users with a systematic and replicable approach for assessing the security posture of their systems and networks. It includes high-level as well as detailed questions related to all industrial control and IT systems.

DHS Cyber Resilience Review
https://www.us-cert.gov/ccubedvp/assessments
The Cyber Resilience Review (CRR) is a complimentary, voluntary program provided by the Cyber Security Evaluation Program (CSEP) within DHS to develop an understanding of an organization's operational resilience and ability to manage cyber risks to its critical services and assets. The CRR pays special attention to protection and sustainment practices with their ten established key domains of cyber resilience, generating a report that summarizes observed strengths and weaknesses in each domain. The report also suggests general guidance or activities to improve the cybersecurity posture and preparedness of the organization. CRR resource guides in the series include these areas: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependencies management, training awareness, and situational awareness.

EEI Principles for Cybersecurity and Critical Infrastructure Protection
http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Principles.pdf
The Edison Electric Institute (EEI) released the principles in 2010 to address the electric utility industry's mandate to provide reliable power. EEI prioritizes collaboration between the state and federal level as well as distinguishes between the priorities of responses to threats and vulnerabilities.

NRECA Guide to Developing a Cybersecurity and Risk Mitigation Plan
https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf
The National Rural Electric Cooperative Association (NRECA) cybersecurity plan addresses general business operations for cooperatives addressing critical infrastructure needs in their systems. The plan is based on the NISTIR 7628, a survey of standards and security concepts specifically for the smart grid.

DOE/NIST/NERC Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline
http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012
The Electricity Subsector Cybersecurity RMP Guideline, resulting from a collaboration between DOE, NIST, and NERC, is a resource geared toward strategic long-term risk management mapped specifically to the electric sector. This resource was developed by DOE, in collaboration with NIST, NERC, and industry representatives. These guidelines can be used to either develop a new cybersecurity program or build upon an organization's existing program.

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
https://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014
The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.1 is an evaluation tool that can be used by electric utilities and grid operators to assess and improve their cybersecurity programs. It is intended to help with implementation and management of cybersecurity practices for IT and OT systems. The ES-C2M2 brings together elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry. The Maturity Model was developed as part of a White House initiative led by DOE, in partnership with DHS as well as industry and other stakeholders.

Recent Legislation

FAST Act
In December 2015, President Obama signed the Fixing America's Surface Transportation (FAST) Act, which authorizes over $300 billion in spending for highway and transportation improvements. Despite its name, this law applies to a range of regulated sectors, including cybersecurity protections for the electric grid. Specific cybersecurity provisions include:

- DOE is designated as the lead sector-specific agency for cybersecurity for the energy sector, and requires the Secretary of Energy to coordinate with DHS and other federal agencies, critical infrastructure entities, and state and local governments.
- Creation of a new information classification of Critical Electric Infrastructure Information (CEII) and requirement for DOE to issue regulations that establish procedures regarding the designation of CEII, prohibit its disclosure, and facilitate voluntary sharing of critical electric infrastructure information among and by federal, state, and local government, as well as the Electric Reliability Organization, regional entities, ISACs, and also owners and operators of critical electric infrastructure.
- The bill also defines an "Electric Security Emergency," which is the presidential declaration that would allow the Secretary of Energy to issue orders to protect or restore reliability of critical electric infrastructure or defense critical infrastructure for the duration of the declared emergency.

- Establishes a renewed information-sharing regime for threats to the grid by requiring DOE, FERC, and other agencies to share timely actionable information regarding grid security with appropriate key personnel of owners, operators, and users of critical infrastructure.
- Establishes liability protections for critical infrastructure entities regarding the sharing or receipt of critical infrastructure information and for any acts relating to its compliance with orders by the Secretary of Energy during an Electric Security Emergency.

PPD-41
https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
In July 2016, the White House issued Cyber Incident Coordination Presidential Policy Directive 41 (PPD-41), which provides principles governing the federal government's response to any cyber incident, as well as the architecture needed to support a broader coordinated response by the Federal Government. PPD-41 creates a single, unifying national policy coordination group, the Cyber Response Group, to coordinate the implementation of the Federal government's policies.

The Directive classifies a cyberattack as either a "cyber incident" or a "significant cyber incident." A "cyber incident" is defined as an event that jeopardizes computer and network infrastructure, physical or virtual, whereas a "significant cyber incident" is defined as an event that is likely to harm national security, the economy, public health and safety, and public confidence, and civil liberties. This Directive clarifies responsibilities when there is a cyber event by designating the U.S. Department of Justice (DOJ) as the lead investigator, DHS as the lead on asset protection, and the Office of the Director of National Intelligence to lead intelligence support activities. The intent is to better safeguard U.S. national interests by improving cooperation and coordination across sectors. This Directive also requires DOJ and DHS to maintain updated contact information for public use to help entities report cyber incidents to the proper authorities.