# Cybersecurity for State Regulators

## With
## Sample Questions for Regulators to Ask Utilities

Miles Keogh
Christina Cody
NARUC Grants & Research

June 2012

Funded by the U.S. Department of Energy

NARUC

The National Association of Regulatory Utility Commissioners

**Acknowledgements and Disclaimers**

The report you are reading was created under the State Electricity Regulators Capacity Assistance and Training (SERCAT) program, a project of the National Association of Regulatory Utility Commissioners (NARUC) Grants & Research Department. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000123.

This report was authored by the Grants and Research Department. Throughout the preparation process, the members of NARUC provided the authors with editorial comments and suggestions. However, the views and opinions expressed herein are strictly those of the author(s) and may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:

Denis Bergeron, *Maine Public Utilities Commission*
Edison Electric Institute
Commissioner Terry Jarrett, *Missouri Public Service Commission*
Annabelle Lee, *Electric Power Research Institute*
Patrick Miller, *EnergySec* & *National Electric Sector Cybersecurity Organization*
NARUC Staff
Thomas Pearce, *Public Utility Commission of Ohio*
Jeffrey Pillon, *National Association of State Energy Officials*
Bridgette Remington, *Vermont Public Service Board*
Alan Rivaldo, *Public Utility Commission of Texas*
Daniel Searfoorce, *Pennsylvania Public Utility Commission*
Christopher Villarreal, *California Public Utilities Commission*

In addition, thanks to Patricia Hoffman and Larry Mansueti of the U.S. Department of Energy for their support of the SERCAT program.

Please direct questions regarding this report to Miles Keogh, NARUC's Director of Grants & Research, mkeogh@naruc.org; (202) 898-2200 and Christina Cody, Program Officer, Grants & Research, ccody@naruc.org; (202) 898-9374.

## Introduction

We often hear reports of cyber attacks in the news, but how serious are the threats to our country's essential utility infrastructure, such as electricity, gas, water and telecommunications?[1] Many State utility regulators have begun asking how to best protect the services, information and data that are valuable to customers, 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 for the electric grid – for State utility regulators, though we hope that it will be useful for 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 sector to develop and implement cost-effective cybersecurity; and
- 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 equipment and systems that communicate, store and act on data. 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 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 handed down from experts. It should evolve as technology, threats and vulnerabilities evolve, introducing the building blocks that stand the test of time while still being flexible enough to meet changing cybersecurity requirements.

*Why Cybersecurity?*

Cyber attacks that cripple the power grid or shut down other infrastructures may be rampant in Hollywood, but to date there have been no reports of a cyber attack successfully crippling critical utility

[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)

infrastructures in the United States – 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 imagine an improbable but realistic scenario.

*Imagine that one Sunday afternoon you turn on the TV to find major news reporting a troublesome, though not devastating blackout affecting a number of areas in your region. In the subsequent days, police and the system operator report that the information about load and generation the grid's regional transmission operator receives had been snuck out – exfiltrated – by parties unknown, and replaced with erroneous data. Dispatchers had to rely on conservative operations in dispatching power plants because they could not trust the data they were receiving without careful review. A few days later, a similar exploit occurs in a vertically-integrated utility's service territory, and soon it is occurring widely and regularly enough, regionally, that careful data review, cross-checking and expensive conservative dispatch become standard practices while the perpetrators are tracked down. Soon thereafter, utility officials report massive denial of service attacks directing tens of thousands of emails an hour to the mobile email systems of their experts and executives, clogging up the flow of information to coordinate response. The situation worsens when substations in the region begin experiencing equipment malfunctions, creating load management problems at the very time that system operators are addressing the system operations data integrity and denial of service problems. Checks of the substations reveal that the firmware in the programmable logic controllers of key sensor devices has been rewritten. It will take ongoing digital forensics to determine what the rewritten firmware even contains, much less how it was overwritten, or by whom.*

*Internal utility emails forwarded to the Public Service Commission warn their staff that malevolent programs are spreading on a peer-to-peer basis within the utility's business process systems looking to exfiltrate customer data, and the utility alerts the regulator that their system may be at risk as well because of the frequency of communications. The Public Service Commission orders an audit of its own internal data systems and IT staff reports that the State system has been successfully penetrated by intruders, but the vendor cannot be certain whether legally protected, commercially sensitive or even detailed utility infrastructure data has been taken. Market-driven system operations are on the shelf for the time being, distribution level reliability is regionally affected and customers are wondering if they can rely on their electric service. Companies and citizens alike are asking hard questions about whether their data is safe. Experts believe they have determined a remedy for breach, but as of now, they cannot be sure who perpetrated the attack and whether more attacks are planned. Service interruptions continue over the next few months, customers' information is still at large and the GDP has contracted significantly after months of stunted power provision across the interconnection.*

This is a pretty bad scenario, but far from the worst case. A dedicated hacker group could accomplish the situation above. A nation-state or well-funded criminal syndicate could theoretically accomplish worse. The more likely scenario is a smaller attack that compromises data without necessarily affecting the operation of the grid. While the above scenario is realistic, the likelier reality may be much easier to address and mitigate. If regulators (and utilities) can imagine the more drastic possibility, it might be easier to imagine – and be prepared 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 is multi-pronged and shared between industry, local, state and federal actors.

*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. While 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 and customer-usage data that may be valuable and desirable to bad actors. [2]

**Increase in Documented IT Vulnerabilities, Per Year**

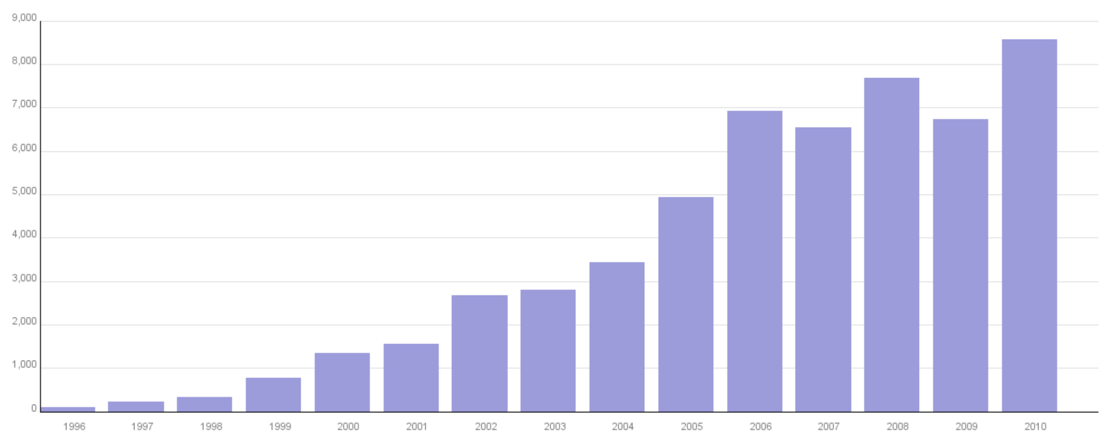



**Figure 1 Data source: IBM X-Force 2010 Trend and Risk Report (for the IT and Telecom sectors).**
**http://www-958.ibm.com/software/data/cognos/manyeyes/visualizations/vulerabilities-per-year**

*Threat Sources*

While 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 cyber attacks from intentionally malicious actors and how to protect against them, although the steps taken to create cybersecure systems are only one part of an all-hazards approach.[3] Cybersecurity must protect 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

[2] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2010: 39.
[3] All-hazards approach takes into account any threat to security, including unintentional or naturally-occuring ones

> *"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*

cannot provide service any better than one flooded with data traffic from a denial of service attack. Other resources[4] may be helpful in establishing an all-hazards approach that addresses risks other than intentional cyber attacks.

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 often the most difficult and least probable outcome. Data theft (or "exfiltration") is a known and ongoing problem. The scope of a cyber attack is also an important consideration. 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 that attack not one component, but multiple components or the network that connects them.

**What Are We Protecting? Three Flavors**

While 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.[5] 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 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 ("dumb") all the way to the firewall and the server ("smart"). Considering how valuable the data of utilities' systems are, the communication, transferences

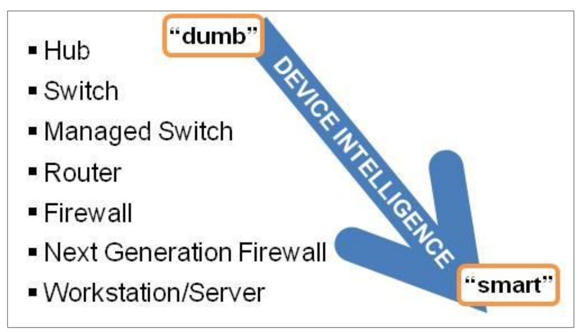



**Figure 2 Spectrum of Device Intelligence**

---

[4] 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

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

and actions based on this data compound its intelligence value. For IT, cybersecurity not only includes software and hardware strategies – passwords, antivirus systems, firewalls, 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.[6]

**Crossing Over from Data Attacks to Physical Impacts: Aurora and Stuxnet**

The most common target of cyber attack is sensitive data, but some examples are emerging 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 the grid.

*Control Systems*

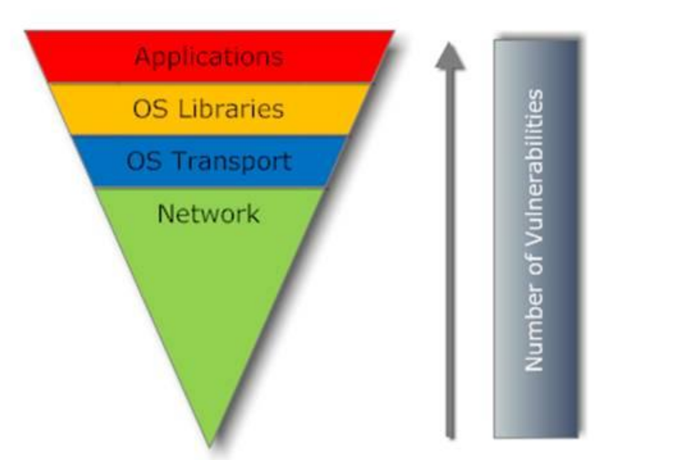
SCADA encompasses systems that monitor and control industrial, infrastructure or facility-based processes, such as utility operations. They include simple functions such as "on/off," sensor capability, communications capability and human-machine interface (HMI) that connects them to people operating 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. With a secure SCADA system, you can trust what your machine is telling you. 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.[7] Even those physically and logically disconnected from other systems may be locally or remotely accessible and have 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.[8] Depending on the situation, some devices may need to be remotely upgradeable, in which case these devices may need capability to use encryption, certificates and authentication. For other devices this may be impractical and access might be required in order 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.

[6] Miles Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," *National Association of Regulatory Utility Commissioners*, May 2009: 6.
[7] NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 31.
[8] 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.

*Smart Grid*

The smart grid is defined differently depending on who you ask, but for this primer it represents the 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. In concept, 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.[9] 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.



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

Smart grid technology touches a number of components – from 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 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.[10]

**Compliance-Based and Risk-Based Approaches to Cybersecurity**

*Using Compliance as a Basis for Cybersecurity*

The owners and operators of critical infrastructure have not been sitting idly by while cyber threats mount. NERC have 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.

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

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:

**NERC CIP Standards**

| Number | Title/Summary | Date | Link |
|---|---|---|---|
| CIP-001-2a | Sabotage Reporting | 02.16.2011 | pdf |
| CIP-002-3 | Cyber Security - Critical Cyber Asset Identification | 12.16.2009 | pdf |
| CIP-002-3a | Cyber Security - Critical Cyber Asset Identification | 05.09.2012 | pdf |
| CIP-002-4 | Cyber Security - Critical Cyber Asset Identification | 01.24.2011 | pdf |
| CIP-002-4a | Cyber Security - Critical Cyber Asset Identification | 05.09.2012 | pdf |
| CIP-003-3 | Cyber Security - Security Management Controls | 12.16.2009 | pdf |
| CIP-003-4 | Cyber Security - Security Management Controls | 01.24.2011 | pdf |
| CIP-004-3 | Cyber Security - Personnel & Training | 12.16.2009 | pdf |
| CIP-004-4 | Cyber Security - Personnel & Training | 01.24.2011 | pdf |
| CIP-005-3a | Cyber Security - Electronic Security Perimeter(s) | 02.16.2010 | pdf |
| CIP-005-4a | Cyber Security - Electronic Security Perimeter(s) | 01.24.2011 | pdf |
| CIP-006-3c | Cyber Security - Physical Security of Critical Cyber Assets | 02.16.2010 | pdf |
| CIP-006-3d | Cyber Security - Physical Security of Critical Cyber Assets | 02.09.2012 | pdf |
| CIP-006-4c | Cyber Security - Physical Security of Critical Cyber Assets | 01.24.2011 | pdf |
| CIP-006-4d | Cyber Security - Physical Security of Critical Cyber Assets | 02.09.2012 | pdf |
| CIP-007-3 | Cyber Security - Systems Security Management | 12.16.2009 | pdf |
| CIP-007-4 | Cyber Security - Systems Security Management | 01.24.2011 | pdf |
| CIP-008-3 | Cyber Security - Incident Reporting and Response Planning | 12.16.2009 | pdf |
| CIP-008-4 | Cyber Security - Incident Reporting and Response Planning | 01.24.2011 | pdf |
| CIP-009-3 | Cyber Security - Recovery Plans for Critical Cyber Assets | 12.16.2009 | pdf |
| CIP-009-4 | Cyber Security - Recovery Plans for Critical Cyber Assets | 01.24.2011 | pdf |

**Figure 3 http://www.nerc.com/page.php?cid=2%7C20**

While 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 upon these standards argue that distribution systems and other key areas where cybersecurity remain a concern to State regulators may not be entirely covered 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 to the CIP standards and still not be secure. Utilities may also be secure but not be compliant to the CIP standards. One is not the guarantee of the other.

*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).[11] 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 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 risk augments traditional "outer wall" approaches to cybersecurity that seek to protect and deny access to the entire system with activities that focus on identifying and addressing the most significant cybersecurity issues. This includes understanding risks, prioritizing them by likelihood, consequence and potential interactions with other risks, and allocating resources accordingly.[12]

## A Few Helpful 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 that regulators be able 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 the following:

- 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*

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 in order 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.[13] This concept was explored in each of the three "flavors" of risk: IT, SCADA and smart grid.

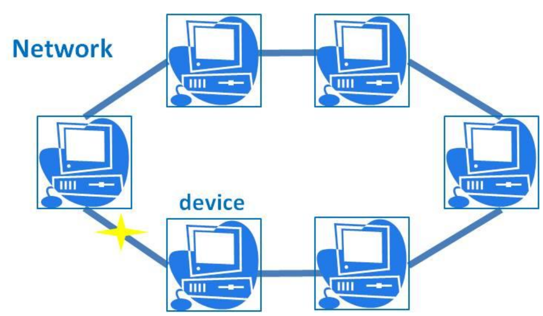



Figure 4 Networks vs. Devices

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

[12] Rich Baich and Ted DeZabala, "Cyber crime: a clear and present danger; Combating the fastest growing cyber security threat," *Deloitte Center for Security & Privacy Solutions* (2010), http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf.

[13] 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.

*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 cyber attack, personnel are skilled in identifying and responding to the impacts. 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 important. These policies, such as the Principle of Least Privilege and "Need to Know,"[14] segregate duties. Securing personnel may also include conducting background checks, ensuring expertise through education,[15] safe and supportive working conditions and finally, continual training to keep expertise up-to-date.[16] 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.

*Defense-In-Depth*

Achieving defense-in-depth requires placing multiple, diverse barriers in front of a potential attacker. Imagine not only locking the outermost doors of an apartment building, but also hiring a guard who checks identification, locking the doors to each apartment, and monitoring loading docks and other points of access that are otherwise unwatched. Likewise, defense-in-depth starts with an overall cybersecurity policy that calls for multiple measures and employs cybersecurity strategies such as identifying authentication and authorization, admission control, encryption, integrity checking, detections of policy violations, data logging and data auditing. For more sophisticated equipment, these strategies may be a straightforward element bundled within the existing software. For older, "dumber" equipment, such as simple control systems, enabling this capacity may be difficult or impossible, necessitating other cybersecurity strategies. 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.

*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 cyber attack should be no less resilient than to a tornado. While 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 in the event that an attack compromises the system, through disaster recovery planning. Plans should be stored in a way that a cyber attack does not affect access to them, such as 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 cyber attacks 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

[14] 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.

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

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

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.

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 assessment. These questions are the basis of evaluating prudence, which we will discuss in the next section. Staff specializing in cybersecurity at commissions are an invaluable resource for drafting the relevant cybersecurity questions for Commissioners to ask utilities during cases. It is very important that questions posed to utilities, however, do not reveal information that could be valuable to a cyber attacker, 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.

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 cyber attacks 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."[17] Key tenets of the resolution encourage Commissioners to prioritize the consistent 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."[18] Keep in mind that ensuring new investments in technologies that are designed with cybersecurity in mind at the front end will create cybersecurity more effectively than adding it to systems later.

The resolution encourages regulators to initiate a dialogue with their utilities to ensure that the utilities are also in compliance with standards. In order to properly review filings to this end, regulators may wish to develop and maintain staff expertise on cybersecurity as it relates to the following topics suggested by NASEO[19]:

1. What is the insider threat and what policies and procedures are in place to prevent intrusion and manipulation?
2. Technical solutions to cybersecurity should account for human behavior, which can be driven by both cultural and psychological factors
3. Nature of the threat from employees, contractors, consultants or anyone with short or long term access to IT systems and knowledge about system vulnerabilities
4. Effect of new systems on consumer behavior – will it strengthen cybersecurity or incite actions to attack the system?

---

[17] NARUC Committee on Critical Infrastructure, "Resolution Regarding Cybersecurity," adopted at the NARUC Winter Meeting of 2010, February 17, 2010.
[18] *Ibid*.
[19] NASEO, "Smart Grid and Cyber Security for Energy Assurance," November 2011: 16.

*Training Resources*

Regulators may wish to invest in training staff on cybersecurity standards and to provide regular updates to training as information changes and technology advances. Internal staff should also be responsible for understanding the cybersecurity of their agency. It may be valuable to have staff members fluent in the concepts of cybersecurity available to serve as a point person for the rest of the staff on all issues relating to cybersecurity. In this way, not only those with an information technology workload familiar with cybersecurity, but 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. In partnership with the National Electricity Sector Cybersecurity Organization (NESCO), NARUC also hosts regular threat assessment teleconferences. 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.

Other resources include:

- *U. S. Computer Emergency Readiness Team's* (U.S. Computer Emergency Readiness Team (CERT) and U.S. Department of Homeland Security (DHS) Control Systems Security Program training: http://www.us-cert.gov/control_systems/cstraining.html
- Pacific Northwest Control System training: http://eioc.pnnl.gov/training.stm
- INL "Red Team / Blue Team" training: http://www.inl.gov/scada/training/advanced_scada.shtml
- Multi-State Information Sharing and Analysis Center (MS-ISAC) http://msisac.cisecurity.org/
- FBI's InfraGard Program: http://www.infragard.net/

*Ask Questions*

Standards, such as the NERC CIP Standards described later in this document, are important but should not be considered to be exhaustive. For example, specific technology standards will not address all the aspects of cybersecurity that are critical, such as high level policies and procedures, that are commonly excluded from standards. Furthermore, existing processes may cover many bulk generation and smart grid aspects of the system, but guidance, standards and other regulations may not currently suffice for elements of the distribution system. It may fall to regulators to ask questions of utilities to determine if there are gaps and facilitate action.

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.

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.

***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 the 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 which 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 cybersecure. 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 cyber attack.

*Prudence*

Ordinarily, a regulator could examine the likelihood and consequence of a potential incident to determine whether the cost of a mitigation strategy was prudent, but with no history of cyber attack and a wide range of potential consequences, there is little guidance that a regulator can turn to. What is a regulator to do?

The below formula is one potential to start from in evaluating prudence by trying to keep the cost of protection lower than the value of what is being protected.

$$P \leq V \leq A$$

Where
V = the value of the components or service provided by the system or data
P = the cost to protect the system/data, and
A = the cost, or risk to an attacker, of the attack.

The value of the service should be greater than the cost of protecting it. These variables can be highly dynamic. For example, the value of keeping electricity flowing to Fenway Park is higher during a Red Sox game than it is in the dead of night after the game is over.[20] Strategies such as loss containment (protecting the overall system, even if some individual components can be compromised) and deterrence (making the attack unprofitable, limited in scope and easily traceable) may be effective alternatives to complete protection. The values assigned to P and V should be based on a risk assessment that utilities have the ability and responsibility to perform with regulatory oversight and auditing. Understanding the cost or risk of attack is an additional tool in assessing the quality of cybersecurity. If expensive protection can be cheaply defeated, regulators may want to explore an alternative investment.

**Developing Expertise: Resources for Regulators to Become Familiar With**

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 between utilities, and potentially PUCs, may be a very important step towards 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/page.php?cid=6|69
The first step for developing cyber expertise is to understand, and where possible engage with, the NERC CIP Standards. These standards already drive a good deal of cybersecurity investments and, as greater coverage is applied to protection of the electric grid, this process will only become more important. 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. The U.S. Department of Energy (DOE) designated NERC as electricity sector coordinator for critical infrastructure protection.

*NIST National Cybersecurity Center of Excellence*
http://www.nist.gov/itl/csd/nccoe-022112.cfm
The National Institute of Standards and Technology (NIST) recently announced the establishment, in partnership with the state of Maryland and Montgomery County, Maryland, a National Cybersecurity

[20] The authors concede this example may be debatable depending on the visiting team and the score.

Center of Excellence. The center will assume $12 million of NIST's 2012 budget and will bring together researchers, user and vendors in targeted tests to address cybersecurity issues.

*NIST Smart Grid Interoperability Panel and Cyber Security Working Group*
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
NIST works collaboratively with industry and government agencies. A wide range of stakeholders and working groups make up the NIST Smart Grid Interoperability Panel (SGIP), responsible, through and open consensus-based process, for interoperable standards aimed at enhancing economic security and quality of life. The SGIP's Cyber Security Working Group (CSWG) works to develop an overall cybersecurity strategy for the smart grid that includes a risk mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The CSWG has developed the NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, available here: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

*The NARUC/NASEO Energy Assurance Guidelines*
Along with organizations like NARUC and the NASEO, which runs an energy assurance program to address state-level coordination on critical infrastructure protection, other national organizations are doing their part to address cybersecurity needs for the energy sector and to serve as resources to government decision makers. Those efforts are detailed in the following. You can learn more about NASEO's Energy Assurance Program here: http://naseo.org/energyassurance/.

*Securities and Exchange Commission Corporation Finance Disclosure Guidance: Cybersecurity*
http://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. 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.[21] This is a vital moment because now a publicly traded company can consider cybersecurity as a business investment.

*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 federal IP programs and the equivalent programs of private sector, State, local, territorial and travel entities. It also operates a forum in which government and critical infrastructure – key resource owners can coordinate critical infrastructure protection.

*EEI Principles for Cybersecurity and Critical Infrastructure Protection*
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 distinguishing between the priorities of responses to threats and vulnerabilities. The *EEI Principles for Cybersecurity and Critical Infrastructure Protection* can be found here: http://www.eei.org/ourissues/ElectricityTransmission/Documents/cyber_security_principles.pdf).

[21] 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.

*NESCO/NESCOR*

To meet the "exponential increase in complexity in securing an ever growing electric grid with an increasing number of stakeholders," NESCO creates a "comprehensive public private partnership to coordinate the efforts in the industry to meet the growing challenge of securing the electric sector." The Energy and Water Development and Related Agencies Appropriations Act of 2010enabled DOE to establish "an independent national energy sector cybersecurity organization." EnergySec and Electric Power Research Institute (EPRI) received fund awards to form NESCO and NESCOR (National Electric Sector Cybersecurity Organization Resource). The two organizations bring together experts to strengthen the cybersecurity posture of the electric sector by working with the DOE Electricity Sector Information Sharing and Analysis Center and industry. More information can be found here: http://www.energysec.org/Websites/energysec/files/Content/840313/2011.02.22_WhatIsNESCO_Webinar.pdf.

*Smart Grid Investment Grant Cybersecurity Requirements*

The American Recovery and Reinvestment Act of 2009 (Recovery Act) authorized funding for the DOE to modernize the electric power grid, including accelerating smart grid development through competitive selection of investment projects in a number of areas, one of which was cybersecurity.[22] This program, called the Smart Grid Investment Grant (SGIG) program, currently supports initiatives like Critical Intelligence Inc.'s Intelligence Training for Targeted Cyber Attacks based in Idaho to train energy sector information security employees to detect and respond to cyber threats (http://www.smartgrid.gov/project/critical_intelligence_inc), and broader programs such as Pepco's "Smart Grid Workforce Training Project" in Washington, D.C., which includes a cybersecurity component through compliance training as part of their overall implementation program (http://www.smartgrid.gov/project/pepco). The SGIG program is just one example of the hardening of the US smart grid currently in place.

*NRECA Guide to Developing a Cybersecurity and Risk Mitigation Plan*

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, found:http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf.

*DOE/NIST/NERC Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*

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. Authorship of the document, which is still in the works, includes industry and utility-specific trade groups. Please find the document here: http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

*Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*

This initiative will serve as a tool for the electric sector to assess their security posture at a given point in time. Driven by the highest levels of the US government the resulting resource should be relevant and important, though as of this writing it remains a work in progress. The latest can be found here: http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012.

[22] www.smartgrid.gov

*Developing Legislation*

Congress has been working on comprehensive legislation for the past four years. Regardless of federal actions in this arena, however, State commissions should be tackling this issue within their jurisdictions to ensure a secure cyber future. The Congressional Research Service (CRS) provides good information on relevant legislation in their latest report, *Cybersecurity: Authoritative Reports and Resources*, which can be found here: http://www.fas.org/sgp/crs/misc/R42507.pdf.[23]

## 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."[24] Therefore, cybersecurity is best approached through a nimble and complex balance of functionality, security and cost. The reality of a "perfect" defense against cyber attack 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 cyber attack 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

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 the ever-evolving threat.

[23] Rita Tehan, "Cybersecurity: Authoritative Reports and Resources," *Congressional Research Service*, April 26, 2012.

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

**Appendix A:**

**National Association of Regulatory Utility Commissioner**

**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 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 cyber attack.

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 Department of Homeland Security? 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. Describe the company's compliance status with NERC CIP-002 through CIP-009. *(Note: Be aware that this may create double-reporting).*

14. 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, ES-ISAC, SANS, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.)?

15. 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)*

16. Compliance as a floor, not a ceiling: are there beyond-compliance activities? Given that there are very little or no cybersecurity standards specified at this point by State regulatory authorities in regard to the distribution portion of the electrical grid, what are you doing to get in front of this?

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

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

**Procurement Practices**

While 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.

19. 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?

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

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

22. 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 Web site hosting?

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

24. 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)

25. 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)?

**Personnel and Policies**

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

26. Is cybersecurity budgeted for? What is the current budget for cybersecurity activities relative to the overall security spending?

27. Are individuals specifically assigned cybersecurity responsibility? Do you have a Chief Security Officer and do they have explicit cybersecurity responsibilities?

28. Does your company employ IT personnel directly, use outsourcing or employ 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 same questions in regard to Operations Technology (OT) (i.e. energy operations) security; larger companies may have separate staffs.)

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

30. 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?

31. 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 which could present a risk to electrical reliability?

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

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

34. 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?

35. 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?

**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.

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

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

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

39. Does the company have equipment dependant 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?

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

41. Discuss what the PUC can do to assist your company in the area of cybersecurity.

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

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

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

45. Are systems audited to detect cybersecurity intrusions?

46. Are records kept of successful cybersecurity intrusions?

47. 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**

| Glossary | |
|---|---|
| **All-Hazards Approach** | Comprehensive approach to security that includes intentional, unintentional, man-made and naturally-occurring threats to the electric grid |
| **Attestation**[25] | The validation of all aspects of a component that relate to its safe, secure and correct operation |
| **Authentication**[26] | Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources |
| **Authorization**[27] | Verifying a user's permissions (after the user had been authenticated) for accessing certain resources or functionality |
| **Bandwidth**[28] | A communication channel the amount of information that can be passed through a communication channel in a given amount of time, usually expressed in bits per second |
| **Boundary protection**[29] | 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**[30] | 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 destroyed, degraded or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system |
| **Connectivity**[31] | 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**[32] | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information |
| **Contingency**[33] | The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element |
| **Control Center**[34] | 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 |

[25] 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.
[26] *Ibid.*
[27] *Ibid.*
[28]ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=5692
[29] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[30] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012: 9.
[31] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6637
[32] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[33] *Ibid.*
[34] NERC, "Glossary of Terms Used in NERC Reliability Standards," 13.

| | |
|---|---|
| | Generation Operator for generation Facilities at two or more locations |
| **Credential**[35] | 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**[36] | 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**[37] | 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 |
| **Cyber Asset**[38] | Programmable electronic devices, including the hardware, software and data in those devices |
| **Cybersecurity Incident**[39] | 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)** [40] | 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)**[41] | 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)**[42] | The cryptographic transformation of data that produces coded text |
| **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 |

[35] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6764
[36] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[37] U.S. Department of Homeland Security, "Critical Infrastructure," (May 23, 2012): http://www.dhs.gov/files/programs/gc_1189168948944.shtm.
[38] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[39] NERC, "Glossary of Terms Used in NERC Reliability Standards," 14.
[40] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.
[41] NERC, "Glossary of Terms Used in NERC Reliability Standards," 18.
[42] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=8119
[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.

| | |
|---|---|
| | that user) where access authorizations to specific objects are assigned based on user identity |
| **Impacta**[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 in order 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** | A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of 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 |
| **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 |

[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.
[51] Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 5.

| | |
|---|---|
| **Management controls**[52] | 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 in order to complete that task, despite clearance level |
| **Network (Computer Network)**[53] | collection of hardware components and computers interconnected by communication channels that allow 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**[54] | The sequence of binary digits transmitted and switched as a composite whole |
| **Physical Security Perimeter (PSP)** [55] | The physical border surrounding locations in which cyber assets, systems or electronic access control systems reside and for which access is controlled |
| **Potential impact**[56] | The loss of confidentiality, integrity or availability that might be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets or individuals |
| **Privileged user**[57] | 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)**[58] | A digital computer used for the automation of electromechanical processes |
| **Resilience** | The ability to restore services rapidly in the event of any disaster |
| **Right-to-Know** | Legal principle that a citizen has the right to know a piece of information about a potential hazard |
| **Risk**[59] | Measure of the extent to which an entity is threatened, typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) 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 |

[52]Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[53] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=6555
[54] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=30770
[55] NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012:36.
[56] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.
[57] *Ibid.*
[58] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.
[59] *Ibid.*

| | |
|---|---|
| **Risk management** | The process 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**[60] | 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**[61] | 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 |
| **Sensitive information**[62] | 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 |
| **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 |
| **Threat** | The potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system |
| **Traffic**[63] | 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 of time |
| **Virus** | An unwanted computer program that replicates itself and spread from one computer to another. "Virus" is often incorrectly used 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 |

[60] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.
[61] *Ibid.*
[62] Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 116.
[63] ATIS Telecom Glossary 2012, http://www.atis.org/glossary/definition.aspx?id=649