Cybersecurity White Paper[1]

Cyril W. Draffin, Jr.

Project Advisor, MIT Energy Initiative

MIT ENERGY INITIATIVE UTILITY OF THE FUTURE

15 December 2016

[1] This document consolidates and slightly augments the cybersecurity, resilience, and privacy sections found in the Executive Summary and Chapters 1, 3, 4, 5, and 9 of the MIT Utility of the Future report issued December 2016. The Appendices of this document provide information not included in the MIT Utility of the Future report.

Table of Contents

Executive Summary……..3

Chapter 1: Introduction: A Power Sector in Transition……5

Chapter 2: Envisioning a Future with Distributed Energy Resources: Cybersecurity, Resilience, and Privacy……..…….7

Chapter 3: The Future of the Regulated Network Utility Business Model: Cybersecurity Preparedness ……..……..…16

Chapter 4: A Comprehensive and Efficient Systems of Prices and Regulated Charges for Electricity Services: Cybersecurity ……..……..22

Chapter 5: Policy and Regulatory Toolkit for the Power System of the Future: Cybersecurity and Data…….…… 23

Appendix A: Cybersecurity Goals for Electric Power Systems....……25

Appendix B: Cybersecurity Threats and Vulnerabilities……28

Appendix C: Regulatory Organizations, Coordinating Organizations, and Standards for Cybersecurity……..…34

Appendix D: Resiliency to Achieve High Reliability……..44

References……..45

Executive Summary

Information and communications technologies are rapidly decreasing in cost and becoming ubiquitous, enabling more flexible and efficient consumption of electricity, improved visibility of network use, and enhanced control of power systems. These technologies are being deployed amidst several broad drivers of change in power systems, including growth in the use of variable renewable energy sources such as wind and solar energy; efforts to decarbonize the energy system as part of global climate change mitigation efforts; and the increasing interconnectedness of electricity grids and other critical infrastructure, such as communications, transportation, and natural gas networks.

Widespread connection of Distributed Energy Resources (e.g. demand response, generation including from wind and solar, energy storage, and energy control devices) will increase digital complexity and attack surfaces, and therefore require more intensive cybersecurity protection. A multi-pronged approach to cybersecurity preparedness is required. System operators must have the capacity to operate, maintain, and recover a system that will never be fully protected from cyber-attacks. Relevant issues that need to be addressed include cloud security, machine-to-machine information sharing, advanced cybersecurity technologies, outcome-based regulation to avoid prolonged outages and increase system resilience, and international approaches to cybersecurity.

Widespread connection of distributed energy resources, smart appliances, and more complex electricity markets increases the importance of cybersecurity and heightens privacy concerns.

- Robust regulatory standards for cybersecurity and privacy are needed for all components of an interconnected electricity network.
- To keep pace with rapidly evolving cybersecurity threats against large and complex electric power systems, electric utilities, vendors, law enforcement authorities, and governments should share current cyber threat information and solutions quickly and effectively.

Maintaining a data hub or data exchange would serve several purposes: securely storing metered data on customer usage, telemetry data on network operation and constraints, and other relevant information; allowing non-discriminatory access to this data to registered market participants; and providing end consumers with timely and useful access to data on their own usage of electricity services. Responsibility for this function should also be carefully assigned, with priority given to data security and consumer privacy considerations.

Utilities will need resilience and will need to be prepared to contain and minimize the consequences of cyber incidents. Future power systems with high penetration of DERs are envisioned to have features that are favorable for their resilient operation. For instance, microgrids, with DERs, are helpful for

resilience, and with "islanding" operations can assist in "black-start" or continued operations if the broader grid goes down due to a cyber or physical incident.

Privacy is also a growing concern, as ever expanding private personal and corporate information is gathered and stored by utilities and their affiliated companies. With expanding connection of electric and telecommunications devices, vastly more information will become available. Data analytics and the opportunity for outside organizations to have access to large quantities of data will increase the amount of information held by electric utilities and their affiliated partners. If electric utility companies expand their services beyond just delivering electricity, by interacting with DER aggregators, for example, specific procedures to protect data breaches and exfiltration of information will be needed.

In summary, key points to consider:

- Industry needs to adopt cybersecurity best practices and develop a risk management culture; cybersecurity regulations are important, but because there is a delay in developing and implementing them, regulations lag behind evolving threats
- Important to rapidly share information about cyber threats, while respecting privacy guidelines
- Good cybersecurity requires skilled teams to understand baseline operations, detect and respond to anomalous cyber activity, reduce the "dwell time" of cyber attackers, and implement layered cyber defenses
- Need to understand and increase system resilience to avoid prolonged outages and recover from cyber attacks
- In the future, utilize advanced cybersecurity technologies, international approaches to cybersecurity, and machine-to-machine information sharing so response to cyber incidents is in milliseconds and not in months

1. Introduction: A Power Sector in Transition

The increasing digitalization of the power sector through the deployment of Information and communications technologies (ICTs) is also embodied in the rollout of advanced metering infrastructure and other network sensing infrastructure in the U.S. and Europe. In the U.S., roughly 59 million smart meters have been deployed, covering over 40% of metered sites (EIA, 2016). In the EU, advanced meter deployments are expected to reach 72% of consumers by 2020 (European Commission, 2016).

The increased digitalization of the power sector is enabling countless new opportunities. Dozens of businesses – ranging from nimble new ventures to powerful incumbents – are offering increased monitoring and control of power networks.

However, the increased digitalization of the power system has created new vulnerabilities. Protecting a nation's electricity grid from cyber attacks is a critical national security issue and an important priority for electric utilities (Campbell, 2015; BPC, 2014). As the December 2015 cyber attack on the Ukrainian power grid demonstrated (EISAC, 2016), electric utilities are vulnerable to attack and will become more so in the next decade as utility systems have more digital controls and operations and metering and resource management systems become more interconnected and complex. The widespread connection of solar, wind, demand-response, and other distributed energy resources with two-way digital controls increases cyber vulnerabilities and requires more widespread and intensive cybersecurity protection. Utilities throughout the world are therefore focusing on resilience and preparation to contain and minimize the consequences of cyber incidents. The increasingly widespread collection and, in certain markets, dissemination of energy production and consumption data is already causing privacy concerns and raising questions over who should own and manage this data.

Furthermore, regulation must account for new risks such as those posed by cyber-attacks on utilities or risks to consumers' privacy.

A modern functioning society requires highly reliable electricity. Electric utilities are vulnerable to cyber and physical attack and will be more so in the next decade as utility systems have more digital and complex controls, and the same digital interconnectedness that increases efficiencies, increase risks. Connection of DERs will increase cyber vulnerabilities. Protecting a nation's electricity grid from widespread cyber or physical attack or electromagnetic pulses are important national security issues, and require wise risk-based analysis and planning by electric utilities. Utilities throughout the world need resilience and contingency planning, to contain and minimize the consequences of cyber and physical incidents.

As utilities gather more information, and with a burgeoning "Internet of Everything" that includes electrical devices in the home, office and industrial facilities connected to the cloud, utilities of the future will need to deal with privacy concerns. Attention to privacy issues may be more important as ever

increasing private personal and corporate information is gathered and stored by utilities and their affiliated companies-- and as new data-centric electric utility business models develop.

2. Envisioning a Future with Distributed Energy Resources: Cybersecurity, Resilience, and Privacy

Cybersecurity threats to the distribution system can be expected to challenge the industry for many decades. Throughout the world, utilities and non-utilities that interact with the grid need resilient systems and must be prepared to contain and minimize the consequences of cyber incidents. Because an increasing quantity of private and corporate information will be gathered and stored by utilities and their affiliated companies, utilities of the future will need to address privacy challenges. Increased use of internet-connected devices in homes, offices, and industrial facilities will exacerbate these challenges, especially since many of these devices store their data in the cloud.

Cybersecurity threats, vulnerabilities, and new approaches

Threats and Impacts

Cyber and physical security threats pose a significant and growing challenge to electric utilities. Unlike traditional threats to electric grid reliability, such as extreme weather, cyber threats are less predictable and therefore more difficult to anticipate and address. The ways in which a cyber-attack[2] can be conducted are numerous and the growing complexity and interconnectedness of electric grids is increasing the number of potential targets and vulnerabilities (MIT 2011; Campbell 2015; Smith et al. 2016; Nourian and Madnick 2015). The attack surfaces of software environments—that is, the different points where an unauthorized user (the "attacker") can try to enter or extract data—are increasing.

Cyber incidents can cause loss of grid control or damage to grid equipment due to deliberate tampering with data, firmware, algorithms, and communications; false data injection into pricing or demand systems; data exfiltration; and ransom demands to restore access to data. Much like the electromagnetic pulses that can be caused by nuclear explosions and major geomagnetic disturbances (including solar flares), widespread cyber attacks are generally high-impact, low-frequency events. Multiple smaller, lower-impact events may occur more frequently. Attacks on the financial and industrial sectors are typically financially motivated, whereas attacks on critical infrastructure systems tend to be politically or ideologically motivated. Future attacks may feature a mix of cyber and physical attacks and may be paired with social action to instill anxiety and fear.

Electric power systems are comprised of cyber systems, physical systems, and people. Failures can originate from physical or cyber attacks and from people acting mistakenly or purposely (i.e., with intent to harm). For instance, DER nodes can be compromised by strategically manipulating generation set points on a distribution feeder (Shelar and Amin 2016). Software attacks can damage variable frequency drives in electro-mechanical equipment to control motor speed and torque. Threats can be both external and internal to the power system. Traditional supervisory control and data acquisition (SCADA) systems, distributed control systems, and programmable logic controllers were designed as closed systems with limited control interfaces, but these technologies are now becoming digitized and are being designed to include more “intelligent” software and hardware components. This increase in

[2] Threats and cyber-attacks can come from a variety of malicious actors, such as foreign nations, terrorist organizations, private firms, external hackers, or internal “bad actors” among system operators, power companies, and vendors. These actors may seek to disrupt grid operations, damage infrastructure, or steal information. They may hire criminal organizations to attack utility grids to disrupt network controls and generation for political reasons, or for economic gain using “ransomware.”

digitization and complexity can create new opportunities for unauthorized outsiders to access, and potentially disrupt, these systems. Future SCADA and distributed control systems may have a secondary diagnostic infrastructure for the purpose of verifying that the system is operating properly and that data are coherent and are not being tampered with. Such a diagnostic center may serve multiple SCADAs in a given region in order to benefit from economies of scale.

Mobile communications connected to utility systems may compound the cyber risks that utilities confront. On December 23, 2015, synchronized multi-stage, multi-site attacks on Ukrainian electric utilities made equipment inoperable and unrecoverable, forcing manual operations to recover and provide power. This served as a "wake up call" to policymakers and regulators to take cyber attacks seriously (Electricity ISAC and SANS Industrial Control Systems 2016). Electric utility cyber incidents, in which systems are breached but not overtaken, continue to occur. Such breaches are necessary precursors to full-fledged cyber attacks, since potential attackers must conduct targeted assessments of specific utility systems prior to launching attacks. The US Cyber Command leadership has stated that cyber attacks by foreign states could cause catastrophic damage to portions of the US power grid (Rogers 2016).

The growth of the Internet of Things (IoT), which can improve efficiency and convenience, also expands vulnerabilities if sufficient cybersecurity and encryption have not been "built in" and vulnerable wireless protocols (e.g., ZigBee) are used. Wirelessly connected IoT devices, including smart light bulbs and other electrical components in a "smart home" or sensors or cameras at an industrial facility, are vulnerable to cyber disruptions and attacks, and could spread malicious code.

The usual purpose of malware that is targeted at electric utilities is to obtain control of a utility's systems. The goal may not be to shut down an entire system but rather to make the system less efficient, disrupt certain regions, game pricing models, gain information about a nation's electricity consumption and industrial operations, or prepare for future attacks.

Associated economic, health, and safety impacts can be large. Lloyd's 2015 Emerging Risk Report indicates that a widespread attack on the US grid, if it were to disable 50 out of the 676 large (over 100 megawatt) generators in a region, could have a $243 billion economic impact and incur more than $20 billion of insurance claims in 30 lines of business (Lloyd's 2015).

On a global level, the average annual cybersecurity budget of energy companies was approximately $3.6 million (US dollars) in 2014, and cybersecurity spending accounted for almost 4 percent of energy companies' information technology (IT) budgets in 2014 (Scottmadden 2015).
In sum, emerging energy markets that enable an active role for DERs and that are based on the near-instantaneous, high-volume exchange of digital information greatly increase the exposure of power systems to cyber attacks.

Organizations and Initiatives

As Table 1 shows, electricity regulatory agencies, electric utility coordinating organizations, and standards agencies all have roles to play in developing cybersecurity standards—for both the United States and Europe.

Table 1: Organizations and Standards Relevant for Cybersecurity in the United States and Europe

	United States	**Europe**
Regulatory Organizations	Federal Energy Regulatory Commission (FERC); North American Electric Reliability Corporation (NERC); state public utility commissions and public service commissions	European Commission (EC; including DG Energy); Agency for the Cooperation of Energy Regulators (ACER); Council of European Energy Regulators (CEER); national regulatory authorities (e.g., UK – Ofgem, Germany – Bundesnetzagentur)
Coordinating Organizations	Electricity Sector Information Sharing and Analysis Center (E-ISAC); Industrial Control Systems – Computer Emergency Readiness Team (ISC-CERT); Electricity Sector Coordinating Council (ESCC); North American Transmission Forum; Edison Electric Institute (EEI)	European Union Agency for Network and Information Security Agency (ENISA); International Council on Large Electric Systems (CIGRE)
Supporting Organizations	Department of Energy (DOE); Department of Homeland Security (DHS)	European Commission Joint Research Centre; European Network of Transmission System Operators for Electricity (ENTSO-E); European Network of Transmission System Operators for Gas (ENTSOG); NATO Cooperative Cyber Defense Centre
Relevant Standards	National Institute of Standards and Technology (NIST) standards and cybersecurity framework; SANS Institute CIS Critical Security Controls	European standardization organizations (e.g., CEN, CENELEC, and ETSI) and CEN-CENELEC Focus Group on Cybersecurity; British Standards Institution (BSI)
International Standards	International Electrotechnical Commission standards; Center for Internet Security critical security controls	

BOX: NIST Cybersecurity Framework

The U.S. National Institute of Standards and Technology (NIST) has established a cybersecurity framework that includes the following objectives (NIST 2014a):

- Identify (institutional understanding to manage cybersecurity risk to organizational systems, assets, data, and capabilities);
- Protect (implement the appropriate safeguards);
- Detect (identify the occurrence of a cybersecurity event, and enable timely responses);
- Respond (activities, to take action regarding a detected cybersecurity event); and
- Recover (restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event).

Cybersecurity programs in all parts of the electric power system need to identify cyber threats and protect operational and IT networks. Poor architecture, some of which was designed decades ago when cyber threats were not as prevalent, can create vulnerabilities, allowing adversaries to obtain initial access, establish reliable inbound and outbound communications, and maintain a persistent presence inside a network. Effective defenders can try to stop these vectors of attack and vulnerable or poorly engineered systems can be replaced if funding allows. Unfortunately, there is no single strategy that prevents all cybersecurity attacks, or eliminates the possibility that DERs will introduce new cyber vulnerabilities (Smith et al. 2016).

Cybersecurity is important to maintain the integrity and correct operation of the electric grid. Thus, minimum cybersecurity regulatory standards are needed for all components of an interconnected network: the bulk power and transmission systems, distribution systems and distributed energy resources, metered points of connection with network users, and internet-enabled devices in residential, commercial, and industrial buildings. All entities that interact with and connect to the electric grid (e.g., DERs, microgrids) should adhere to minimum cybersecurity standards, not only those entities, such as utilities, that are registered with the North American Electric Reliability Corporation (NERC). Non-traditional energy providers and electricity service providers, including DER aggregators, should be obligated to address cyber risks because their actions (or inactions) could have a dramatic impact on the overall security of the electric grid.

In 2013, the US government issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity.[3] Other cybersecurity standards, regulations, and practices in place in the United States include NERC's Critical Infrastructure Protection Standards Version 5, a cybersecurity framework developed by the National Institute of Standards and Technology (NIST), and the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model.

In July 2016, the European Commission issued a communication on "strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry.[4] The European Commission also created the "Energy Expert Cyber Security Platform" (EECSP) with the aim of

[3] President Obama's Executive Order 13636 on Improving Critical Infrastructure Cybersecurity was issued on February 12, 2013. It is available at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[4] The European Union (European Parliament and the Council) Directive 2016/1148, concerning measures for a high common level of security of network and information systems across the Union, was issued on July 6, 2016. It is available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

providing guidance to the Commission on policy and regulatory direction EU-wide. The first European legislation on cybersecurity, the Network and Information Security (NIS) Directive, was issued in July 2016 and entered into force August 2016. The directive provides legal measures to increase the overall level of cybersecurity in the EU by increasing cybersecurity capabilities in member states, enhancing cooperation on cybersecurity among member states, and requiring operators of essential services in the energy sector to take appropriate security measures and report incidents to national authorities. Once implemented, European consumers, governments, and businesses will be able to rely on more secure digital networks and infrastructure to reliably provide essential electricity services. However, significant coordination on the part of member states is required to reach similar levels of cybersecurity across all of the European Union. Moreover, although the NIS is a promising first step, more explicit cybersecurity regulations and best practices will need to be implemented in Europe.

A better understanding of the costs of meeting future standards for cybersecurity and resilience is required. In the United States, there is currently no single central authority for cybersecurity preparedness. The Federal Energy Regulatory Commission (FERC) and NERC have authority over cybersecurity standards development and compliance for the bulk power system, but there is no formal regulatory oversight of compliance with cybersecurity standards at the distribution system and for smaller aggregations of DERs. Some state public utility commissions have started to address cybersecurity challenges at the distribution level, but more decisive actions are required. Similar cybersecurity regulatory oversight and action is needed in Europe and in other parts of the world. For the millions of DER components that will ultimately be deployed, direct control by utilities is not feasible; rather, a hierarchical approach is necessary for utilities to interact with these widely dispersed cyber-physical systems. DER security specifications should be developed, updated, and used by utilities and other non-traditional utility entities for all types of installations. A National Electric Sector Cybersecurity Resource report titled “Cyber Security for DER Systems” provides common technical security requirements for autonomous cyber-physical DER systems, DER energy management systems, utility- and retailer-operated ICT, and DER interactions with ISOs, RTOs, and energy markets (Cleveland and Lee 2013). Additional cyber guidelines that address DER actors, logical interfaces, and logical interface categories, can be found in the NIST Interagency Report on “Guidelines for Smart Grid Cybersecurity” (NIST 2014b).

The International Electrotechnical Commission and its technical committee have also developed security recommendations and standards for information exchange for power systems. The Commission’s 2016 technical report on “Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems” provides cybersecurity recommendations and engineering and operational strategies for improving the resilience of power systems with interconnected DER systems (IEC 2016).

Advancements in DERs create new ways of interacting with the power system. For instance, electric vehicles may contribute to cyber risk in the distribution system when smart or price-sensitive charging strategies would require bi-directional communications between charging and distribution control systems. Moreover, these systems must support many vehicle types and therefore many communication protocols, which makes filtering and network analysis much more difficult. Additionally, like portable USB drives, electric vehicles can carry mobile viruses between grids or into homes, defeating network separation defenses. Therefore, manufacturers of hybrid or electric vehicles and autonomous driving features will need to integrate cybersecurity in the design phase.

The first step to defend against cyber attacks is to develop a robust cyber risk management culture. Each organization must start by identifying and classifying the risks it faces, and by undertaking a

security assessment of its infrastructures. Once risks have been identified and classified, action plans must be developed and periodically reviewed. Well-vetted frameworks and policies for physical disaster management and recovery already exist; these can serve as precedents for approaching cyber risk management.

Actions

To address cybersecurity breaches (a precursor to possible cyber attacks), network planners and operators need to understand what constitutes baseline or "within-band" operations, and need to be prepared to detect and respond to anomalous cyber activity. As DER capacity increases, digital automation expands, and more interconnected services are provided, many new cyber "attack surfaces" will be created. Utilities and DER providers need approaches to defend against such attacks, reduce the "dwell time" of attackers, implement multiple layers of cyber defenses ("defense in depth"), and recover from cyber and physical attacks.

As more utility and operational systems employ "cloud-based" services and cloud computing for data storage and processing, enhanced and non-conventional cybersecurity methods will be required. If data from multiple utilities and entities are stored in the cloud, new cybersecurity approaches will be needed. Regular scans for known cyber vulnerabilities and malware at all levels of generation, transmission, and distribution will be required. Relying only on Internet perimeter security will fail to protect distributed networks. In these cases, enhanced encryption for individual software components, hardware, and data will be even more important. Because enhanced analytics and artificial intelligence can help identify "anomalous" or "out-of-band" behavior, these potential solutions merit attention. Both cybersecurity and dynamic cyberattack strategies will evolve, and compliance with NERC, FERC, and European Commission regulations will be only the starting point for more robust and proactive cybersecurity systems. Governance institutions and industry coordinating organizations to ensure continuous improvement in cybersecurity best practices for the industry as a whole will be required. These institutions can serve a role analogous to that of the Institute for Nuclear Power Operations, which promotes high levels of safety and reliability in commercial nuclear reactors.

The US Electricity Information Sharing and Analysis Center coordinates rapid information exchange about cyber incidents, providing coordination for more than 80 percent of the United States, a significant portion of Canada, and parts of Mexico. Electric utilities and other key organizations in Europe, Asia, South/Central America, and other parts of the world would benefit from a wider and more rapid exchange of cybersecurity information. Work is required to develop a framework that balances this sharing of information with the need to respect the individual concerns of participating bodies. To keep up with rapidly evolving cybersecurity threats against large and complex electric utility networks, there is a need for electric utilities, vendors, law enforcement agencies, and governments to share current cyber threat information and actionable intelligence. Established organizations in the United States, such as the Electricity Information Sharing and Analysis Center (E-ISAC), the Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT), and intelligence agencies need to improve communications and continue to conduct emergency response exercises such as GridEx and Cyber Guard. In Europe, established organizations that enable trust-based sharing of security data and information, such as the European Energy Information Sharing & Analysis Centre (EE-ISAC), need an even broader mandate, more robust mitigation strategies, and approaches for coordinated recovery from cyber attacks. Ideally, robust information sharing across agencies and international organizations will generate trust among these agencies and organizations and contribute to the efficient processing of critical information (Choucri et al. 2016).

Providing cybersecurity for the electric grid requires developing a risk management culture; understanding the characteristics of baseline or "within-band" operations; rapid sharing of information about cyber threats; and active, skilled, and coordinated teams to detect and respond to anomalous cyber activity, defend against cyber attacks, reduce the "dwell time" of cyber attackers, and implement layered cyber defenses.

Resilience with DERs[5]

The 9/11 attacks and Hurricanes Katrina and Sandy in the United States, the Tohoku earthquake and tsunami in Japan, the cyber attack on Ukraine's power grid in 2015, and other terror incidents and natural catastrophes demonstrate the critical importance of resilience for energy systems. The concept of resilience has been interpreted differently in different disciplines, such as psychology, physics, ecology, and engineering. In the United States, President Obama's 21st Presidential Policy Directive[6] defines this term in the context of energy infrastructure: "resilience is the ability of critical infrastructure to prepare for and adapt to changing conditions and withstand and recover rapidly from all hazards, which include natural disasters, industrial accidents, pandemics, cyber incidents, sabotage, acts of terrorism, or destructive criminal activity." Many jurisdictions around the world view resilience as an important characteristic of electricity networks, and are incorporating resiliency measures into national and regional legislation—another example is the European Commission's Programme for Critical Infrastructure Protection.[7] Practices that improve resilience at the system level have been in place for decades. In the 1970s, a classification system was introduced to characterize the operating state of the power grid: normal, alert, emergency, *in extremis*, or restoration. Which classification applied in a given situation depended on operational conditions (as measured by, for example, frequency, voltage, power flows, etc.) and external conditions (such as weather). Since then, contingency analysis has been used in unit commitment dispatch. Moreover, operating power reserves have been created to respond to undesirable imbalances of demand and supply, load curtailment has been used to respond to severe imbalances, and strategically located generators have provided black-start capability to restore power after a blackout. Other good practices include stockpiling spare transformers and developing detailed response plans.

Power systems are changing and DERs will provide new opportunities to improve resilience system-wide. In future power systems, the current network topology (meshed transmission network and radial distribution network) will extend to integrate microgrids at the customer or community level (Ton and Smith 2012). If designed correctly, this build-out is expected to help isolate failures, provide alternative pathways for avoiding component failures, resolve local failures before the entire network is exposed

[5] Section on "Resilience with DERs" was prepared by Pablo Duenas-Martinez, Postdoctoral Associate, MIT Energy Initiative.

[6] President Obama's "Directive on Critical Infrastructure Security and Resilience" (Presidential Policy Directive–21) was issued on February 12, 2013.

[7] See Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM (2006) 786 final at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=en. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection. SWD (2013) 318 final. 28 August 2013 at https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

to instability, and maintain continuity of service even under extremely severe conditions. Microgrids, when combined with DERs, can help provide resilience. With the use of "islanding" operations, microgrids can assist in black-start or continued operations if the broader network is compromised due to a cyber or physical incident.

A small number of success stories in Japan have demonstrated the potential of distributed energy systems to maintain power delivery under extreme conditions. Ropponggi Hills is an area in downtown Tokyo that self-provides electricity, heat, and cooling. Service in this area was uninterrupted on March 11, 2011 following the 9.0 magnitude earthquake and tsunami, and Ropponggi Hills helped restore service in other areas. Its Sendai microgrid was able to serve most of the nearby university campus as well as critical facilities such as a hospital. Likewise, in the United States, distributed energy systems and microgrids proved advantageous in the aftermath of Hurricane Sandy (Hampson et al. 2013; Marnay et al. 2015).

However, the presence of DERs also raises new challenges for resilience. More DERs entail more complex network configurations and operations. In networks with significant active DER participation, ICT systems will have to coordinate thousands (or hundreds of thousands) of decentralized devices alongside hundreds (or thousands) of centralized generators. This alone can increase system vulnerability to extraordinary events. The power system of the future will consist of both cyber and physical assets that are tightly integrated, and all of these assets must be protected. But mere protection is not sufficient. As described in the previous section, a resilient power system must also include the ability of the cyber-physical grid to withstand and recover from malicious and inadvertent cyber and physical attacks. The traditional approach of redundancy does not work if a cyber attack disables all similar units.

Utilities need to carefully plan for extraordinary events. Utility mutual response agreements for responding to natural disasters may not work well for cyber attacks of unknown duration and scope. Increased deployment of DERs will require utilities to operate in a more complex environment, and may lead to common failure modes if the same DER software configurations are used across regions or nations. Utilities need to be able to operate in a partially manual mode, disconnected from the main grid, if digital controls and telecommunications are unreliable following a cyber attack. Spare equipment programs in the United States, such as the Spare Transformer Equipment Program, SpareConnect, and Grid Assurance can improve grid resilience. Similarly, resilience should be formally considered in EU planning, directives, and legislation, and should be improved at the regional level.

To meet the novel challenges posed by cyber threats, utilities are developing a tiered approach to sustain service during an attack and restore service once disruption occurs. These measures include developing control mechanisms that will not provide the full functionality of regular systems but can sustain limited vital operations and maintain "fall-back" mechanical controls (Stockton 2016). Because the control center is the nerve center of the power system, and because its resiliency is extremely important, the computer hardware and software in the energy management system should be designed to withstand failures and degrade gracefully when necessary. The control center must be protected from physical as well as cyber attacks, and a backup control center should be available. Adjacent control centers (for example, the PJM Interconnection and the Midwest Independent Transmission System Operator are adjacent systems in the United States) should partially back each other up (NRC 2012).

Resilience is important in minimizing interruptions of service due to extraordinary events such as cyber attacks. Enhancing resilience requires detailed planning, effective mutual assistance

agreements, and thoughtful use of DERs and microgrids. Privacy is an ongoing concern.

Privacy

Privacy is an increasingly important issue for individuals, companies, and utility systems. Hence, the potential for widespread adoption of DERs and IoT technologies to exacerbate privacy concerns is an important topic. Vastly more information will become available with the increasing connectivity of electric and telecommunications devices. Data analytics and the opportunity for outside organizations to improve user experience and generate additional revenue will increase the amount of information that is held by electric utilities, DER service providers, and other service providers. If data are held in cloud storage and are accessible to multiple people and organizations, maintaining privacy will become more challenging. Current privacy restrictions, encryption requirements, and information disclosure requirements vary by country and region (within the United States, disclosure requirements also vary by state) and by the type of data held. If electric utilities begin to collaborate more with device control system aggregators, electric car owners, and vehicle charging aggregators, specific procedures to protect data breaches and information exfiltration will be required. The challenge is to simultaneously protect legitimate customer expectations of privacy, be a good steward of data, and apply analytics to create additional value for consumers.

In Europe, a recent revision of General Data Protection Regulation 2016/679 makes Data Protection Impact Assessments mandatory under certain conditions. These assessments are a key instrument to enhance data controllers' accountability.[8] The European Commission's energy group (DG Energy), the Joint Research Centre, and industry developed a Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems to help utilities assess smart grids when evaluating privacy and data protection.[9]

[8] See General Data Protection Regulation 2016/679 (Ref. European Union 2016/679) at eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679).

[9] Available at ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

3. The Future of the Regulated Network Utility Business Model: Cybersecurity Preparedness

Challenges in Cybersecurity, Privacy Regulation, and Standards

The proliferation of DERs and ICTs in electricity networks will continue to increase the vulnerability of these systems to cyber attacks. The grid is a cyber and physical system, and future threats may involve both dimensions. Strong cybersecurity regulations, standards, and best practices are needed for all levels of the system—including the bulk power system (central generation and transmission), distribution systems, DERs, smart meters, and electrical devices with Internet connectivity in industrial, commercial, and residential buildings.

The grid is a cyber and physical system, and future threats may involve both dimensions. Strong cybersecurity regulations, standards, and best practices are needed for all levels of the system—including the bulk power system (central generation and transmission), distribution systems, DERs, smart meters, and electrical devices with Internet connectivity in industrial, commercial, and residential buildings.

Cybersecurity investments suffer from a type of market failure in which the benefit of secure operations is shared among electricity providers and network users, but each actor's private incentive to invest in adequate cybersecurity preparedness is too low to justify the cost. Network utilities, many of which face slow or negative electricity growth and relatively uncertain financial futures, tend to make investments that increase financial returns rather than spend money on cybersecurity, which has limited direct financial benefit. Network utilities will therefore require additional regulatory incentives to invest in adequate levels of cyber protection.

Current cybersecurity regulations vary across transmission and distribution systems, across regions, and across utility-owned and independently owned DERs. In the United States, the North American Electric Reliability Corporation (NERC) has developed cybersecurity regulations at the bulk power and transmission levels (NERC 2016). In Europe, the first European legislation on cybersecurity, the Network and Information Security (NIS) Directive, entered into force in July 2016 (European Union 2016a). Regulations at the distribution-system level (including DERs and customer connection points) are lacking, therefore a baseline set of cybersecurity standards for all distribution networks is needed. Continuous improvements in best practices will also be required to meet evolving cyber threats. Achieving good cybersecurity in the future demands good governance as well as regulation because rule-making is not sufficiently nimble to keep up with evolving threats. Instilling good governance is difficult. Industry organizations such as the Institute of Nuclear Power Operations have been reasonably successful for the nuclear industry, but there is currently no equivalent for the cyber and physical security of electricity networks.

In addition to strengthening cybersecurity standards and regulations, privacy regulations also may need to be updated to address issues raised by the influx of DERs and Internet-connected devices. As network utilities gather more detailed information about network users and as the number of Internet-connected devices in distribution networks rises, privacy concerns may be exacerbated. Regulators may therefore need to adopt new approaches to privacy regulation. For example, European Union privacy regulations approved in April 2016 give citizens control of their personal data and create a uniformly high level of data protection (European Union 2016b).

Finally, new precautions and standards are needed to protect against cyber attacks. Since the proliferation of DERs and ICTs in electricity networks will continue to increase the vulnerability of these systems, strong cybersecurity regulations and standards are needed for all levels of the power system.

Cybersecurity Preparedness

Widespread connection of DERs will increase digital complexity and attack surfaces, and therefore require more intensive cybersecurity protection. A multi-pronged approach to cybersecurity preparedness is required, including enhanced information sharing on cyber threats and possible responses. Although cybersecurity regulations and standards have been adopted, they will need to be updated and enhanced. Moreover, because cyber attack strategies will evolve, complying with regulations will only be a starting point; it will be necessary to improve cyber defense best practices continually. The power grid is an inherently open system. From a cybersecurity standpoint, the population of relevant cyber and physical devices is extremely large. Every electric vehicle, building energy management system, smart thermostat, and electrical device with a connection to the Internet and every interconnected infrastructure—gas, communications, water—could potentially be used in an attack on the stability of the power grid. A challenge is to have the capacity to operate, maintain, and recover a system of subsystems and devices that will never be fully protected from cyber attacks. In the longer term, relevant issues that need to be addressed include cloud security, machine-to-machine information sharing, advanced cybersecurity technologies, the possibility of adding chief information security officers to distribution companies, outcome-based regulation to avoid prolonged outages, and international approaches to cybersecurity.

Although some DER systems may have been deployed without robust cybersecurity protections, future cybersecurity protection standards and privacy concerns can become a barrier to the deployment of DERs until clarification is provided regarding what cybersecurity standards will be required and how much meeting those standards will cost DER systems and DER aggregators. In addition, evolving privacy concerns and regulations need to be taken into account alongside deployment of aggregated demand-response and other DER systems that gather large amounts of private and corporate energy-use information. The privacy and ownership of users' data must be protected by DER owners and operators using appropriate systems and safeguards.

Current approaches for information sharing in Europe

Information sharing can make DERs more reliable because cybersecurity and interface problems—and potential solutions—can be communicated more quickly to mitigate widespread issues. Information sharing will play a key role in the development and deployment of cybersecurity standards and solutions in the European Union. Fortunately, certain initiatives are already under way. For example, a network of national Computer Security Incident Response Teams (CSIRTs) has been established under the NIS Directive. The CSIRTs network will be composed of representatives of the member states' CSIRTs and CERT-EU (Computer Emergency Response Team for European Union institutions, agencies, and bodies). The European Union Agency for Network and Information Security (ENISA) will actively support the cooperation among CSIRTs. Among other tasks, the CSIRT network will support the exchange of information on CSIRTs' services, operations, and cooperation capabilities. A detailed list of the CSIRT network's tasks is provided in article 12(3) of the NIS Directive (European Union 2016a).

Several other initiatives exist in Europe at the national and international levels to share information on risks, vulnerabilities, and threats. For example, the European Commission has established the Energy Expert Cyber Security Platform and the Thematic Network on Critical Energy Infrastructure Protection, and it has financed the Distributed Energy Security Knowledge (DENSEK) project. One of the deliverables of the DENSEK project was the establishment of the European Energy - Information Sharing & Analysis Centre, which plays an important role in cybersecurity information sharing in the energy sector in Europe. Over time, cybersecurity information sharing could be augmented and coordinated with the support of other organizations, such as the European Network of Transmission System Operators for Electricity.

In the United Kingdom, cybersecurity information sharing is achieved via a government-industry consortium known as the Energy Emergencies Executive Committee Cyber Security Task Group, as well as via the Cyber Security Information Sharing Partnership, an initiative that allows users to share real-time cyber threat information.

Expanding cybersecurity regulation in the United States and Europe

To improve cybersecurity in the United States, state regulatory commissions could work together to establish standards applicable to distribution utilities and modeled on the existing NERC Critical Infrastructure Protection standards. This would remove the uncertainty surrounding what cybersecurity standards will be applied to DERs. Using an approach similar to NERC, authorities could announce regulations that apply to distribution utilities (and large distributed generators) along with a date that the regulations would come into effect. State public utility commissions would be responsible for new critical infrastructure protection guidelines applicable to distribution utilities. These cybersecurity standards would apply to DERs owned by both utilities and non-utilities. Harmonizing regulatory standards at the

transmission, distribution, and end-user levels would contribute to economies of scale and reduce the cost of cybersecurity preparedness.

In Europe, the European Commission encourages member states to make the most of NIS coordination mechanisms. Building on those, the commission will propose how to enhance cross-border cooperation in the case of a major cyber-incident. Given the speed with which the cybersecurity landscape is evolving, the commission will also evaluate ENISA, which will possibly lead to the adoption of a new mandate. Common coordinated standards are likely to be more effective at reducing risks for involved member states than piecemeal guidelines that vary by state.

Longer term approaches for building cybersecurity resilience

To address the long-term cybersecurity challenges faced by network utilities, a multifaceted approach is recommended.

First, cybersecurity regulations or standards should consider network and market operations that are performed in the cloud in order to make data interfaces consistent, clear, and secure. Performing network and market operations in the cloud with consolidated information would require enhanced security, robust monitoring, and artificial-intelligence and machine-learning technologies to monitor out-of-norm activities. Individual DER operators and aggregators would provide secure, authenticated data to a private or hybrid public/private cloud data repository and network utilities with appropriate cybersecurity protections, and market operators would assess the veracity of the information. In this way, operations would be consolidated; instead of relying on separate systems with different protocols and control software, this plan would ensure all data and controls pass through major portals. If executed well, this type of configuration could lead to more secure and efficient operations and would enable DER providers to interact with and utilize utility data. However, the integration of DER communications with network operations could create risks of wider outages in the case of attack; therefore, it is recommended that DERs be required to have adequate built-in security measures before connecting to the grid and to cloud systems that control network and market operations.

Second, trusted capabilities for sharing threat information from machine to machine will need to be deployed in the United States and Europe to enable timely monitoring of and response to cyber incidents that can develop within minutes. However, high-speed monitoring and information transfer significantly increases the need to ensure that threat data and response plans are coming from verified official sources.

Third, enhanced cybersecurity technologies are needed to address the evolution of more sophisticated cyber attacks and cyber technology and reduce the likelihood of successful attacks on DERs and the grid. Such technologies include advanced encryption, programs to ensure information integrity, artificial intelligence and behavioral analysis, moving target techniques to randomize cyber system components, and cyber-secure architecture (including processor memory safety, unauthorized application denial,

and compiler validation). With the layering of industrial Internet of Things technologies on top of the existing infrastructures (including decades-old programmable logic controllers and remote terminal units), security technologies will be needed for disaggregated single-purpose devices. Model-based engineering and virtualized risk simulators can be used to evaluate the security and performance of utility systems.

Fourth, each network utility should have a chief security officer—an executive responsible for addressing key cybersecurity, physical security, and privacy challenges; for ensuring that regulations are understood and followed within the organization; and for ensuring that DERs and control systems are safely connected to the Internet. This executive can ensure that cybersecurity and physical controls are not insurmountable barriers to connecting DER systems to the grid. Corporate boards of directors also need to understand and evaluate cybersecurity-related risks, governance, and operations; review results of security audits; evaluate cyber-event prevention and recovery plans and operations; act when a cybersecurity breach is known; and evaluate cyber-insurance options. Companies need to establish formal cybersecurity risk management processes in which senior managers and board members are engaged. All parts of the corporation, from the board to the general workforce, need training to understand and address these risks.

Fifth, cyber attack avoidance and mitigation regulation could be considered to augment baseline cybersecurity standards. To achieve increased levels of innovation with the goal of avoiding prolonged outages over a broad geographic area due to a cyber attack, explicit financial incentives—outside of the core remuneration framework—could be provided for network utilities to spearhead pilot projects. An "input-based" financial incentive, whereby pilot projects are capitalized and included in the regulated asset base (in a cost of service regulatory context) could work to mitigate holistic security risk and minimize the chance and impact of high-cost, low-probability events such as a widespread cyber attack. These regulations will bring enhanced security concerns into utility reliability and disaster recovery planning. In addition, because regulators face an extremely difficult task when asked on a state-by-state basis to evaluate the reasonableness and effectiveness of utility security expenditures, there could be requirements for utilities to maintain private cyber insurance and to provide external validation of utility cyber governance. If a successful cyber attack caused a network utility to face a penalty, there would be a penalty cap, such as that used for utility supply, that limits the penalty to a percent of the company's remuneration so as not to send a company into bankruptcy.

Finally, because of the substantial impact of electricity, including from DERs, on the economic stability and health and welfare of citizens worldwide, an international approach to cybersecurity is recommended as part of a comprehensive strategy. A global international agreement would be difficult to achieve; however, an intergovernmental initiative such as this would not be without precedent. Examples include the Budapest Convention on Cybercrime, the Chemical Weapons Convention, the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, and the Montreal Protocol on Substances that Deplete the Ozone Layer. To achieve

international support, an organization such as the United Nations, working with nation states, worldwide electric utilities, Internet service providers, and groups such as the Organization for Security and Co-operation in Europe and international law enforcement organizations, could initiate this effort and determine how to monitor any agreement that was reached.

4. A Comprehensive and Efficient Systems of Prices and Regulated Charges for Electricity Services: Cybersecurity

Cybersecurity-related costs

Computation of appropriate prices between DERs and TSOs/DSOs requires consideration of cybersecurity. TSOs/DSOs need to monitor DER suppliers and assure malware or cyber-attacks are not introduced into the TSO/DSO control or pricing systems. Cyber risks can come from DER control systems, demand response systems, dispatchable energy storage systems, smart meters, and other DERs that communicate with TSO/DSO control systems. As DERs participate in the price formation with buying and selling bids into different markets, digital connections to utility pricing and accounting systems need to be sufficiently protected and monitored. Fixed charges can be used to recover the cost of meeting protection standards.[10]

Determination of appropriate communication system interfaces between DERs and TSOs/DSOs also requires consideration of cybersecurity. Data interface and protocol standards, communication architectures, and advanced control algorithms should be established that are consistent, have strong encryption, and require multi-factor authentication, and security by design introduced progressively in all new equipment. Communications between DERs and TSOs/DSOs need to be monitored for anomalies to avoid unexpected disruptions of power, and DER control and systems that interface to TSOs/DSOs should allow approved upgrades to allow enhanced data interface standards and to fix identified cyber security flaws. TSOs and DSOs could provide secure communications equipment, for charges agreed-upon with regulators, which later would need to be allocated to customers.

---

[10] For example, U.S. North American Electric Reliability Corporation (NERC) critical infrastructure protection standards, European Commission standards, state Public Utility Commission standards, or National Electric Sector Cybersecurity Organization Resource suggested requirements. Source: National Institute of Standards and Technology. Interagency Report on "Guidelines for Smart Grid Cybersecurity" NISTIR 7628, Volumes 1-3, September 2014.

5. Policy and Regulatory Toolkit for the Power System of the Future: Cybersecurity and Data

Finally, as the power system becomes more digitalized and as DERs proliferate, distribution systems will face new cyber threats that today's regulations are not adequately prepared to manage.

Recommendation 1: Proactively address current and potential future cybersecurity issues.

Most of the recommendations in this report rely on or imply a greater degree of digitalization and interconnectedness in the power system. This sets the stage for our final recommendation concerning distribution system regulation.

Widespread connection of DERs will increase digital complexity and attack surfaces, and therefore requires more intensive cybersecurity protection. A multi-pronged approach to cybersecurity preparedness is required. Providing cybersecurity for the electric grid requires developing a risk management culture; understanding the characteristics of baseline or "within-band" operations; rapid sharing of information about cyber threats; and active, skilled, and coordinated teams to detect and respond to anomalous cyber activity, defend against cyber attacks, reduce the "dwell time" of cyber attackers, and implement layered cyber defenses. System operators must have the capacity to operate, maintain, and recover a system that will never be fully protected from cyber attacks. Relevant issues that need to be addressed include advanced cybersecurity technologies, machine-to-machine information sharing, cloud security, regulation and implementation of best practices to avoid prolonged outages and increase system resilience, and international approaches to cybersecurity.

Proactive regulation and best practices to address cybersecurity threats are critical as the power system becomes increasingly digitalized.

Recommendation 2: Carefully review and implement best practices in the management of power sector data.

To facilitate level-playing field competition between aggregators (including retailers), DER providers and a diversity of competitive agents active within distribution systems, a core function is becoming increasingly important: that of data platform or data hub.

Experience in retail markets in Europe and elsewhere have demonstrated that all market participants need equal and non-discriminatory access to a degree of customer information sufficient to facilitate a level-playing field for competition. Likewise, timely and non-discriminatory access to data on network conditions and operation and planning decisions, as well as information on network customers, could be an important facilitator for competition among DER service providers and aggregators.

As more data is collected from increasing connectivity of electric and telecommunications devices, more attention needs to be given to who has what rights to use the data, and for what purposes. Utilities,

DSOs, Data Hubs, and data managers have responsibility to act as data stewards to protect customer privacy and the security of the information to which they have unique access, and to abide by government regulations and good practices, such as the European General Data Protection Regulation and the US Federal Trade Commission's Fair Information Practices. Privacy and security safeguards also need to be implemented by third parties that provide analytics and have access to raw power sector data.

***Regulators should review and carefully assign the responsibility for data management*, while considering multiple goals, including non-discrimination, efficiency and simplicity. Data on customer usage, telemetry data on network operation and constraints, and other relevant information must be securely stored and made available in a non-discriminatory, timely manner to registered market participants. Consumers must be provided with timely and useful access to data on their own use of electricity services. Data privacy, data protection, and data rights will require increasing attention.**

Appendix A: Cybersecurity Goals for Electric Power Systems[11]

Customers and nations desire highly reliable electric utility grids with short term limited outages, limited catastrophic failures that causes electricity to be lost for many days in wide swaths of a country, and allows an electric utility to effectively operate in an environmentally-conscious future. Following are series of goals for good cyber operations:

- Be able to operate in an environment where cyber attacks occur. In the future electric utility operating control and business systems will have to operate in conflicted cyberspace, where penetrations of systems will occur and constant vigilance is needed. The concept of walls, moats, and firewalls used for network defense are no longer effective, and are not likely to be in the next decade. Over many centuries the world has not been able to stop physical attacks and crime, so there is no reason to believe we will be able to stop all cyber attacks and crime.

- Reduce an attackers' access to our systems. To do so, over the next decade it will be important to consider "dwell time"— the time from when an adversary or an unwanted external party "infects" or penetrates a computer system until the time the software or access is deleted. Also we want to avoid lateral movement, when a person penetrating a specific electric utility system or subsystem gets to move to or control other internal systems. We want to get more internal visibility to improve on the current situation when frequently organizations do not learn they have been compromised for many months or years-- until problems occurs or an outside organization like the US Federal Bureau of Investigation points out the compromise.

- Seek proper treatment. There is an analogy of getting sick. Everybody gets exposed to germs and viruses, and the human body mounts internal defenses from the immune system, which give people resiliency to external infections and threats. People want to practice good hygiene, avoid infection when possible, and maintain monitoring systems, but it is impossible to avoid all contact with infections, so some sickness is inevitable. People seek treatments when exposed, and when appropriate seek experts for advice. The same is true for cybersecurity— computer systems get exposed to germs, viruses, and other attacks; get infected; and need treatments to expel the attackers and mitigate the impact of the attack.

- Provide Cyber Defense in Depth, so there are coordinated layers of protection. This is especially important when new attack vectors exploit "zero day" (previously unknown) vulnerabilities, and attacks are implemented. We need protection from both external attackers and inside attackers. As the diversity within utilities that have relied on Programmable Logic Controllers, Remote Terminal Units, and analog systems decreases, and as utilities move to consolidated and integrated systems using a small number of vendors with products having the same firmware in deployed in many systems, the risk of widespread attack using shared vulnerabilities in multiple electric utilities could increase.

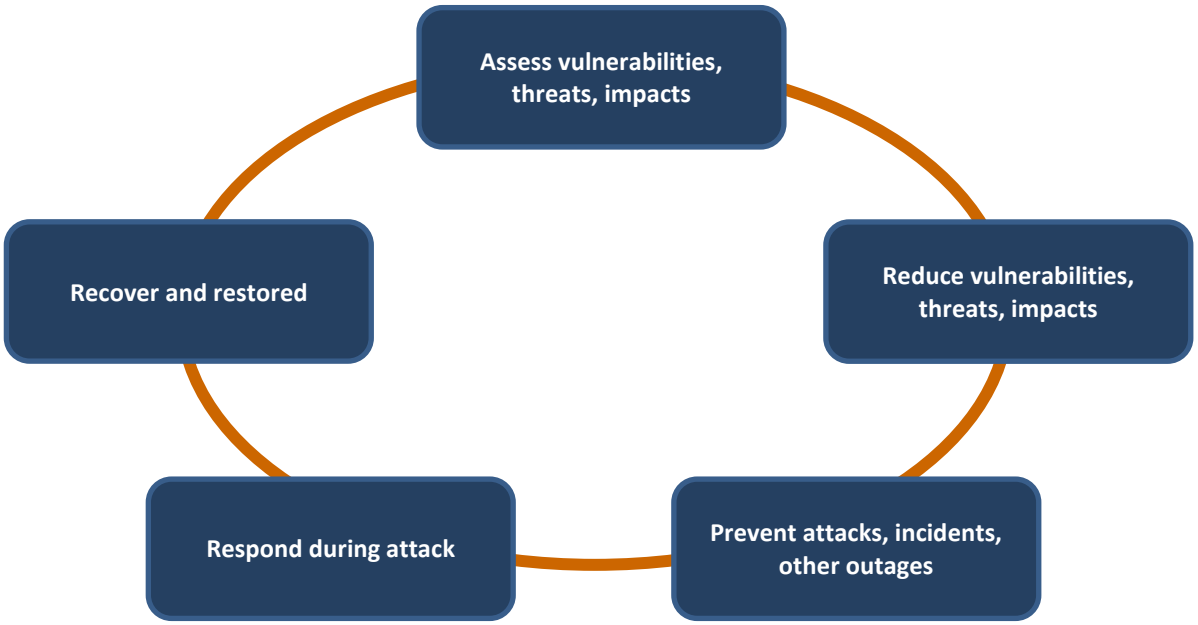
- Use continuous monitoring and compliance with cybersecurity best practices, and not rely just on standards that are only checked infrequently (for instance semi-annually).

- Develop systems so cybersecurity is more like storms and hurricanes where we can track and predict consequences, and less like earthquakes where we have very little warning when they will occur.

[11] Ideas in this chapter drawn from multiple sources.

- Address the entire Security Life Cycle (Identify, Protect, Detect, Respond, and Recover). Vulnerabilities need to be assessed and reduced, attacks prevented when possible, effective speedy response when attack occurs, and a thoughtful plan to recover and restore operations as shown in the Cybersecurity Life Cycle, shown in Figure 1.

Figure 1: Cybersecurity Life Cycle



- Establish effective response systems, and to improve upon multiple soloed cybersecurity tracking and alert systems that can result in a flood of alert messages requiring human intervention without clear prioritization (which can result in the most important issues not being addressed in a timely way).

- Prepare resiliency plans to respond to low likelihood but high impact attacks.

- Promote innovation as utilities become more complex and evolve into an increasingly decentralized power sector, in a time of rapid change in information systems and technology. The traditional focus of regulation has been to achieve competitive markets and cost reductions in network activities. Innovation and more frequent "refresh" of information systems and their security is likely to be required.

- Have a workable system for determining the appropriate cost expenditures and cost allocation for a reliable, secure and resilient electrical system. Considering that electric utilities are "Profit and Loss" organizations, there is a disincentive to spend funds on cybersecurity if they are not included in the rate base or required by regulation.
    - Need to consider the range of costs for cybersecurity, and who pays for improved cybersecurity of the electric grid including the distribution system. If electric utilities are being "squeezed" by decreasing electricity demand and shareholder return expectations, need to have a driving force to assure sufficient cybersecurity is funded. To address these issues, tools need to be developed to measure impact of cyber expenditures, and groups like the MIT Sloan School (IC)3 program is trying to address.

  - Mechanisms will be needed to get electric utilities to use best cyber practices and follow the new and evolving cybersecurity frameworks such as under development by the U.S. National Institute of Standards and Technology.
  - Have risk based expenditures, with special attention paid to the few most-critical systems and the vulnerabilities with the most critical exposures.
  - There is a regulatory challenge to address extensive long-duration cybersecurity outages, where the probability is very low although the cost may be very high, by adopting appropriate and not cost-prohibitive cybersecurity measures.

- Address information privacy and security for utility customers and utilities. The future electric grid will collect, communicate, and store detailed operational data from tens of thousands of sensors as well as electricity-usage data from tens of millions of consumers. Issues arise from protecting the data and making data available only to people who need them for legitimate purposes. Key questions that to be addressed by the utility industry and regulators include:

  - What data are we concerned about?
  - How do we determine who should access that data, when, and how?
  - How do we ensure that data are appropriately controlled and protected, and at what level of fidelity?
  - How do we determine who owns that data?
  - How do we balance privacy concerns with the business or societal benefit of making utility data available?

- Establish a community or eco-system to consider risk management, establish priority of action, support other electric utilities, and keep knowledge and cybersecurity technology integrated and current in the face of rapidly evolving threats, and a large number of possible solutions.

Appendix B: Cybersecurity Threats and Vulnerabilities[12]

The electric power system is comprised of cyber systems, physical systems, and people. Failures can come from physical and cyber attack or from people who do not do the right thing, either by omission or with intent to harm. Threats can be both external and from insiders. Cyber attacks will happen:

- Cyber attacks can come from anywhere
- Cyber threats cannot be eliminated, only mitigated
- Mitigation costs money – and although it is hard to measure the benefit, the economic costs of losing power for extended periods can be very large
- Cybersecurity ought to be high priority for government, Public Utility Commissions, and utilities

Threats are becoming more dangerous, sophisticated and persistent. Complexity is adversary's most effective weapon in the 21st century. New information technology product features increase attack surfaces. As utilities have moved from electromechanical and analog devices to interconnected digital devices, risk of external penetration has increased. Source of threats include:

- Potential external threats from terrorist organizations that hire criminal organizations to attack European or US utility grids (effecting network controls and generation)
- Potential threat from insiders (e.g. people inside the external firewall of utilities and grid operators can affect all parts of the system), and some insiders can be "co-opted" without them knowing Insider threat

One of the challenges of maintaining reliability is cybersecurity. An attack by a disgruntled employee or adversary such as a nation state, could have sudden and very negative economic and social consequences if it knocked out the flow of electricity for hours or days, or even months.

Power distribution systems are at potential risk to nationwide hazards from both natural and manmade threats. Two studies commissioned by the North American Electric Reliability Corporation (NERC) assessed these risks: High-Impact, Low-Frequency Event Risk to the North American Bulk Power System (2010), and Severe Impact Resilience: Considerations and Recommendations (2012). Both studies focused on risks with the potential to cause catastrophic impacts on the electric power system, but which either rarely occur or (in some cases) have not yet occurred but occur in the future. These risks include coordinated cyber, physical, and blended attacks; the electromagnetic pulse effects created by the high-altitude detonation of a nuclear weapon; and major natural disasters like earthquakes, tsunamis, large hurricanes, pandemics, and geomagnetic disturbances (GMD) caused by solar weather (e.g. solar flares).

Physical Vulnerabilities

Source of physical vulnerabilities include:

- Weather (e.g. falling trees, hurled objects, intense wind/lightening)
- Earthquakes (e.g. see below for potential risk of New Madrid fault)
- Physical attack (e.g. California physical attack by rifles on substation)
- Physical theft of electricity (e.g. in countries in various parts of the world, e.g. India or Italy)

Physical Hazards pose risks of creating long-term, wide area outages. The New Madrid Seismic Zone in the U.S. exemplifies these risks. The New Madrid fault roughly parallels the Mississippi River, and produced of a 7.7 earthquake in 1812. A recurrence of that earthquake today (which was the focus of a 2011 U.S. National Level Exercise) would damage or destroy many hundreds of electric substations, high voltage transformers and transmission lines, generators, and other grid components over a multi-state region including Illinois, Indiana, Missouri, Arkansas, Kentucky, Mississippi, Tennessee, and potentially other States. The Department of Energy assessed that such an event

[12] Issue presented in this section were drawn from multiple sources including Campbell, Richard J., Congressional Research Service, "Cybersecurity Issues for the Bulk Power System." June 10, 2015

would not only disrupt power in the New Madrid region but far beyond, with outages potentially affecting 100-150 million people.

Cybersecurity Vulnerabilities

Cybersecurity refers to all the approaches taken to protect data, systems, and networks from deliberate attack as well as accidental compromise, ranging from preparedness to recovery.

Cybersecurity is an important element of information systems enabling the Utility of the Future. For instance, a survey of electric utility executives *in "Strategic Direction: U.S. Electric Industry"* (*Black & Veatch, 2014)* found that cybersecurity was the fourth-highest concern for electric utilities, behind reliability, environment regulation, and economic regulation. Utilities want to avoid systems failure and cyber breaches that require expensive recovery (in both costs and reputational damage). However, the financial incentives to invest in cybersecurity are limited because the electric utility business model does not provide strong incentives to spend substantial sums on providing a very robust infrastructure that is not required for regular distribution and supply of electricity for events that cannot be consistently predicted. This is a challenge in addressing massive electricity outages where the probability may be low but the costs may be very high. Table 2 shows potential impact of complexity and DERs on cybersecurity vulnerabilities:

Table 2: Cybersecurity Vulnerabilities with Complexity and Distributed Energy Resources

Location of Increased Cybersecurity Vulnerabilities	Potential Impact of Complexity (more complex digitally interconnected grid & active management)	Potential Impact of Distributed Energy Resources
Electricity Generators • More external monitoring & dispatching & DERs	*x*	*x*
Electrical/Grid Control Systems (transmission & distribution) • More digital interfaces, sophisticated SCADA, load balancing, voltage frequency control, monitoring	X	X
Smart Meters • More digital connections and customer interfaces	X	*x*
Pricing, Bidding, and Billing Systems • More active generator and customer interfaces & customer privacy issues (including complexity with time of day pricing)	X	*x*

X = Large Impact *x* = Small Impact

The Bipartisan Policy group's report (2014) stated that Cyber threats to North America's electric grid are growing, making electric grid cybersecurity an increasingly important national and international issue. The Federal Bureau of Investigation (FBI) noted that cyber attacks are eclipsing terrorism as the primary threat facing the United States.

As cyber attacks become more frequent, energy systems are increasingly being targeted. The Industrial Control Systems Cyber Emergency Response Team (ICSCERT), which is part of the U.S. Department of Homeland Security (DHS), responds to cyber incidents. Threats can come from a variety of malicious actors, such as foreign nations, terrorist organizations, private firms, external hackers, or internal "bad actors" among system operators, power companies, and vendors. These actors may seek to disrupt grid operations, damage infrastructure, or steal information.

It is possible that electrical wires to users can be a vector for attacking military and industrial targets. Some military organizations are concerned that the electrical lines or the systems providing energy monitoring may provide a pathway for sophisticated attackers to gain access to military systems and information.

Control System Vulnerabilities

Example Vulnerabilities include:

- Widespread use of DERs that increase cybersecurity vulnerabilities unless best practices are used by DERs and utilities (for network controls and generation, and to lesser extent generation and pricing, and bidding and billing systems)
- Use of advanced technologies such as synchrophasers that rely on Global Positioning systems for accurate time sensitive information could be attacked by "spoofing" the GPS signal
- Vulnerabilities demonstrated by prior cyber attacks on energy systems including Stuxnet, Aurora, Slammer, Night Dragon, phishing attack Shamoon (Bipartisan Policy Center, 2014. p20)
- Use of cloud, mobility applications, and Internet of Things (technologies that are advancing quickly and are being deployed)
- Errors or tampering with data communication among control equipment and central offices that cause loss of grid control resulting in complete disruption of electricity supply over a wide area can occur as a result of.
- Sabotage of Power Grid by attacking SCADA systems and substation operations through internal or external communications channels

The challenges to maintain cybersecurity of the control systems for the electric grid come from several characteristics of the future grid:

- New control systems and processes: Large amounts of information generated from grid operations at the individual utility and consumer level will require new control and management systems and processes. These systems will be integrated to provide better response, to integrate intermittent renewable power, and to match supply and demand, but the more sophisticated and interconnected systems also will introduce vulnerabilities.
- Components: The electric grid will be composed of components from multiple suppliers, with multiple interfaces and protocols, and relying on multiple standards both in the United States and Europe. Replacing traditional mechanical control systems may reduce mechanical part failures and increase ability to control systems, but some older mechanical systems were more isolated from cyber attacks.
- Continuous transition: The information and communications technologies used in the grid will continue to change at a faster rate than utilities can change components in the grid (or upgrade embedded firmware and security systems in the components). This will result in incompatibilities and security vulnerabilities between existing and new equipment, and the risk that monitoring or billing systems cyber penetrations can result in control system manipulation.
- Increased data communications: Information interconnections throughout the electric grid will introduce new cybersecurity risks and challenges, to both local and wide-scale grid systems.
- Speed of software updates: In Information Technology business systems, software updates are frequently made weekly (or more rapidly). In industrial control systems they

may only be done annually, and for some components never (until the components are replaced)

It is probably not possible to avoid attack on US or European electric utility system from sophisticated nation states or their operatives (after the electric utility systems have been breached electronically). Therefore, coordinated cyber and kinetic response by US or European governments, as well as electric utilities, may be necessary to deter those cyber attacks

Electrical System Vulnerabilities from Electromagnetic Pulse

- Risk of Electromagnetic pulse from an airborne-exploded nuclear device frying electronic equipment is substantive, although that attack has not be made on a commercial electric utility
- Are there affordable ways of partially mitigating or recovering from such an attack feasible, other than burying large amounts of equipment and spares?

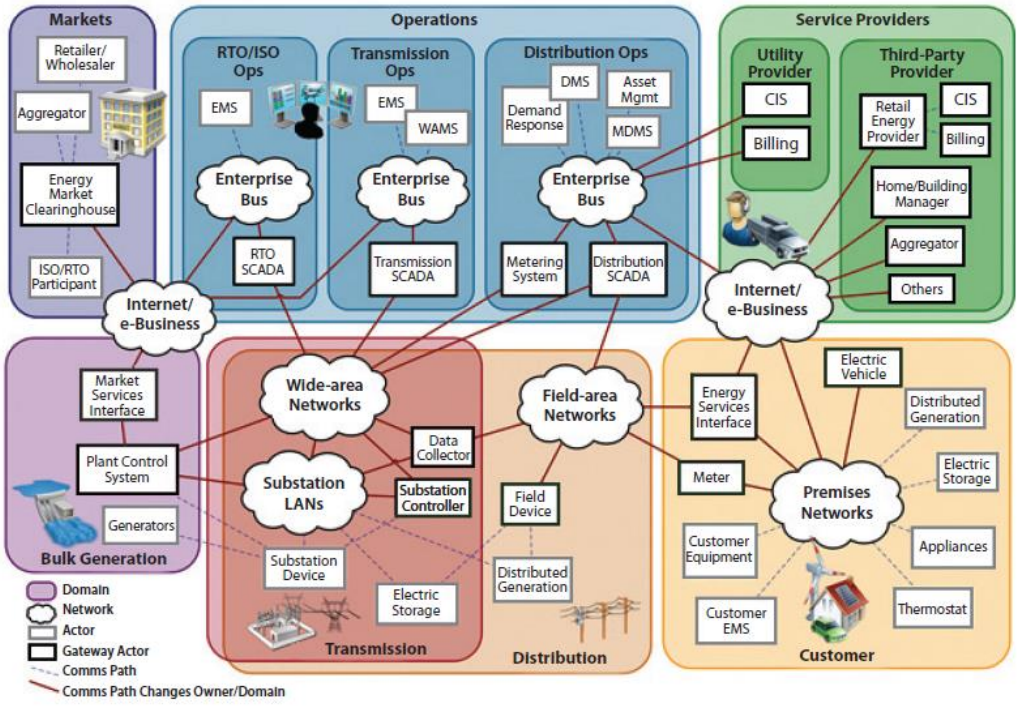
Utility Electricity Pricing System and Billing Vulnerabilities

For billing systems, false data injection or manipulating pricing systems could skew the market and potentially create a windfall in electricity pricing

Data Communications Vulnerabilities

More communications results in more vulnerabilities. Different types and generations of components must be interoperable. Decisions to standardize on protocols are complex and require input from a variety of stakeholders, as illustrated in Figure 2. More analysis on Data Communications (and Figure 2) can be found in the MIT Energy Initiative 2011 Future of the Electric Grid report. (MIT 2011)

Figure 2: Detailed Communications Flows in the Future Electric Grid



Source: National Institute for Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, special publication 1108 (Washington, DC: U.S. Department of Commerce, 2010), 35, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Privacy and Data Confidentiality Vulnerabilities and Problems

- Data confidentiality breaches, both personal and corporate, can provide information for identity theft, corporate espionage, physical security threats (for example, through knowing which homes are vacant), and terrorist activities (for example, through knowing which power lines are most important in electric distribution).
- Smart meter tampering can result in sudden power outages or incorrect billing. Smart meters are capable of recording and transmitting electricity-usage information every few minutes. These and other measurement devices installed in homes and businesses will become even more capable in the future, potentially achieving almost continuous monitoring of the electric usage of lighting systems and other electric appliances. The policy issues these technological advances raise include questions about what data should be collected, why and by whom, how collection and storage should be paid for, who controls such data, and how it should be protected.
- Privacy breaches can be used for identity theft or local crime
- Electric vehicle movements can be tracked using charging station information. It is possible to remotely control vehicles (without permission) due to cyber penetration of vulnerabilities in monitoring or entertainment systems

Observations on Vulnerabilities

A number of observations can be made regarding vulnerabilities

- Cybersecurity is like Chess, which was developed in 6th century India, because both involve multiple paths of attack and defense. Both require thinking ahead on what might happen, but in the cybersecurity challenge, new pieces and moves are always being added.
- The Critical Infrastructure Protection Standards from NERC are usually five years old before they are adopted, and are insufficient for strong cybersecurity protection. Addition cybersecurity best practices, using NIST framework and SANS controls are necessary to achieve sufficient cybersecurity.
- Defense is harder than offense, because only one major well-orchestrated cybersecurity attack is needed to disrupt. For institutional reasons, too often in cybersecurity, it seems the attackers are better organized and collaborate more closely than the defenders.
- Vulnerabilities tend to be at the “seams” of interconnected systems and organizations when gaps and inconsistencies of security policies or data transfer can result in opportunities for external parties to access and modify the systems
- Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization’s infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem. The more extensive use of cloud computing, mobility applications and interconnections, and Internet of Things will increase potential vulnerabilities.
- Enemies on our network have capacity to do harm. Iran attack Saudi Aramco affected approximately 35,000 hard drives. Multiple organizations have reported that China has infiltrate our electrical network
- Bold successful cyber attack would create a supercharged political environment for power restoration operations-- and Federal, state and local leaders will create urgent and incessant demands for information on Estimated Time of Restoration, restoration priorities, and how scarce restoration resources are being allocated. Commissioners and utilities can expect political leadership engagement, with attendant problems for setting and communicating. This requires prior planning for managing crisis-driven restoration issues.
- The question is not whether there will be attacks and disruptions, but when and how severe will they be—and how quickly and effectively utilities can respond to the outages caused.

Cyber attacks could be considered in three levels of intensity, which require different levels of support:

1. Basic attacks: Utilities are concerned about reputation risk and do not make money if not producing electricity due to outage, so they will continue to take basic steps of cyber protection and used of cyber defense tools

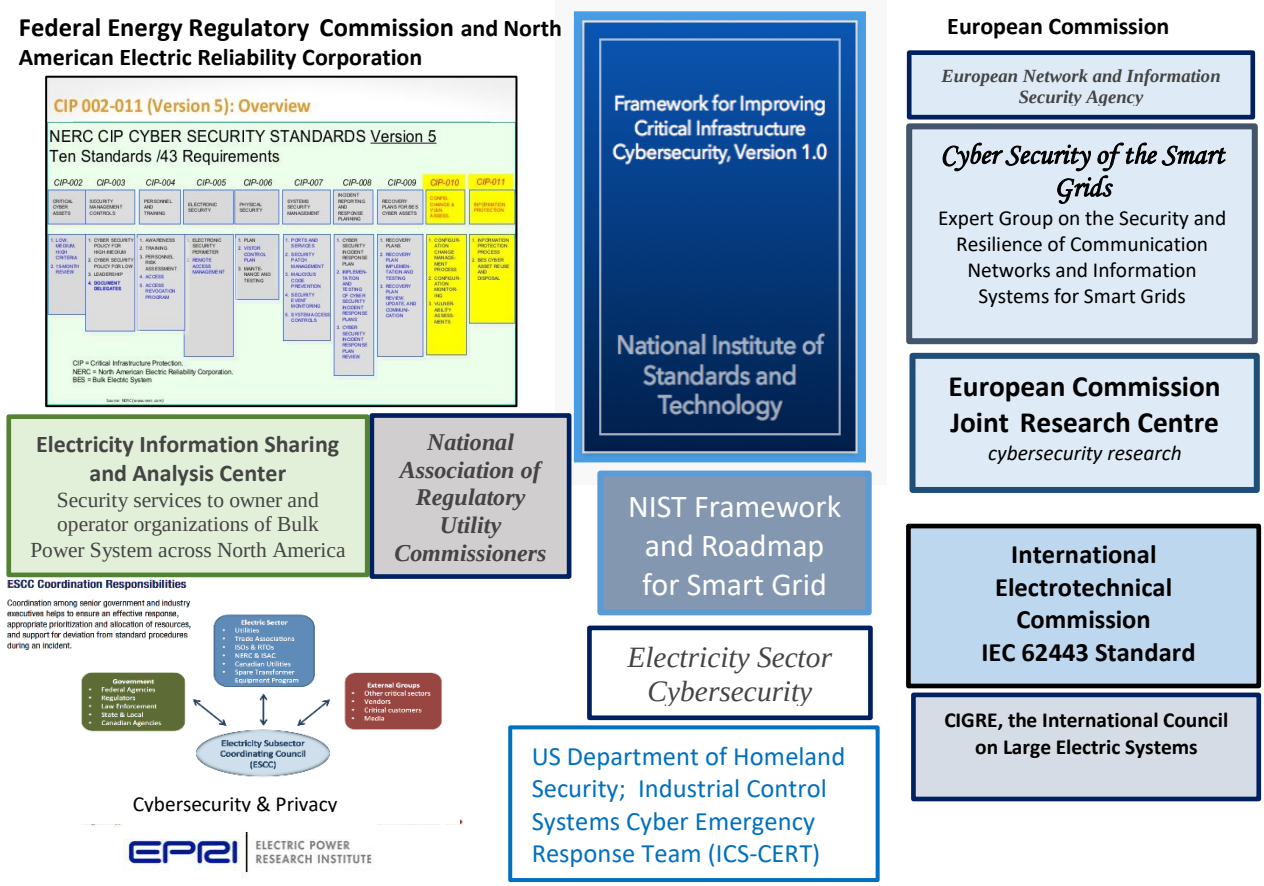
2. Intense attacks: Utilities need information sharing on attacks/attackers and advice on how to stop attacks from central government authorities and a network of utilities. Most utilities will need to augment current staff to defend against and respond to intense attack.
3. Nation-state attacks: Utilities will need assistance to respond to Advance Persistent Threats (APT) from the US and other governments to withstand well-funded and perseverant cyber attackers

Appendix C: Regulatory Organizations, Coordinating Organizations, and Standards for Cybersecurity[13]

To address vulnerabilities, multiple approaches can be taken. Operational approaches to address cybersecurity risks include deployment of improved cyber-hardened information systems, and consistent adherence to cyber standards. Regulatory approaches to address cybersecurity risks include regulatory changes that require and compensate utilities for improved cybersecurity performance.

A summary of electric utility regulatory organizations, electric utility coordinating organizations with a role in cybersecurity and resiliency, and relevant standards, for different parts of the world are found in this document and Figure 3. (Note: Figure 3 visually presents US organizations on the left and in the center, and European and International organizations on the right; there are no flows shown or order to the placement of the organizations.)

Figure 3: Organizations Involved in Cybersecurity for Electric Utilities in the US and Europe



The bulk electric power system has mandatory and enforceable standards for cybersecurity. The U.S. Energy Policy Act of 2005 (P.L. 109-58) gave the Federal Energy Regulatory Commission (FERC) authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for

[13] This section provides background information. Because all the information in this section may not be current, check with the individual organizations for the most current information.

critical infrastructure protection (CIP) which are updated considering the status of reliability and cybersecurity concerns for the grid.

The U.S. bulk power system is already subject to mandatory federal reliability standards that include some cybersecurity protections. Critical infrastructure protection (CIP) standards are developed by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). These standards cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans. While standards provide a useful baseline level of cybersecurity, they do not create incentives for the continual improvement and adaptation needed to respond effectively to rapidly evolving cyber threats. Distribution facilities generally operate outside of FERC jurisdiction. In some cases attacks at the distribution-system level could have consequences that extend to the broader grid. Also some regulatory groups do not have the ability to enforce implementation and can only make recommendations. Cybersecurity at both the bulk power system and at the distribution system levels. (Bipartisan Policy Center, 2014, p 9-10)

U.S. Presidential Executive Order 13636[14]

In February 2013, the White House issued an executive order titled "Improving Critical Infrastructure Cybersecurity" and an accompanying Presidential Policy Directive. Executive Order 13636 aims to improve the sharing of information regarding cyber threats between government and private actors, including classified information. The executive order also requires DHS to identify critical infrastructure that could be vulnerable to cyber attack with potentially catastrophic regional or national consequences, and to assess the privacy and civil liberty risks associated with its programs. Finally, the executive order directs the NIST to develop a Cybersecurity Framework that addresses cyber risks and is applicable to multiple sectors and industries. In February 2014, NIST released Version 1.0 of its Cybersecurity Framework.(NIST 2014). The framework attempts to build on existing standards and practices in critical infrastructure industries to enable companies to: "1) describe their current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders." While the framework and its updates are voluntary, it could eventually form the basis for future state or federal regulations or otherwise set the "standard of care" for purposes of assessing liability in the wake of a cyber event.

Several of the key organizations and their missions with regard to electric power sector cybersecurity are profiled below.

U.S. Federal Energy Regulatory Commission (FERC)[15]

FERC is responsible for ensuring the reliability of the bulk power system. FERC separately established the Office of Energy Infrastructure Security (OEIS) to deal with cyber and physical security.

Under authority granted by the Energy Policy Act of 2005, FERC designated the North American Electric Reliability Corporation (NERC) as the Electricity Reliability Organization responsible for developing mandatory and enforceable reliability standards in the United States. NERC also has been formally recognized by applicable government authorities in Canada. These reliability standards address issues relevant to the operation of existing, new, and modified bulk-power facilities, including critical infrastructure protection (CIP).

North American Electric Reliability Corporation (NERC)

[14] Exec. Order No. 13,636, 78. Fed. Reg. 11,739 (Feb. 19, 2013)

[15] A substantial portion of the material on, FERC, NERC, and E-ISAC came from Bipartisan Policy Center Report, "Cybersecurity and the North American Grid," February 2014 (which provides additional references). See the organizations' web sites for current details.

NERC security guidelines identify actions that electricity subsector organizations should consider when responding to threat alerts received from the Electricity Information Sharing and Analysis Center (E-ISAC) and DHS (for U.S. organizations) or from Public Safety Canada (PSC) (for Canadian organizations); define the scope of actions that organizations may implement for specific response plans; conduct assessments of vulnerability and risk to identify critical facilities and functions; and categorize the vulnerabilities and risks associated with those facilities and functions. NERC physical security guidelines address substations, generating facilities, control centers, and transmission infrastructure.

NERC also issues email alerts to disseminate actionable information necessary to ensure the reliability of the bulk power system. NERC alerts are categorized into three levels: industry advisories, which are purely informational and do not require a response; recommendations to industry, which recommend specific actions by registered entities and require a response as indicated; and essential actions, which identify specific actions necessary for reliability and require a response as defined in the alert. CIP standards (version 5/6) cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans.

NERC's role in information sharing extends to its operation of the E-ISAC (see section below).

NERC participates in a number of other activities aimed at improving electric grid cybersecurity. For example, NERC's Grid Security Exercise (GridEx) allows companies to validate their response to simulated physical and cyber incidents. More than 200 organizations from the United States, Canada, and Mexico participated in the 2013 GridEx, making it the largest sector-specific security exercise. NERC's annual Grid Security Conference (GridSecCon) provides an opportunity to discuss emerging cyber threats and best practices and provides training opportunities. NERC also participates in a number of cybersecurity initiatives led by DHS, DOE, and Canadian government organizations.

NERC's Critical Infrastructure Protection Committee (CIPC) is responsible for its physical security and cybersecurity initiatives. CIPC consists of both NERC-appointed regional representatives and technical subject matter experts, and serves as an expert advisory panel to the NERC Board of Trustees. It has standing subcommittees in the areas of physical security and cybersecurity. The CIPC also oversees the Electricity Information Sharing and Analysis Center (E-ISAC).

Electricity Information Sharing and Analysis Center (E-ISAC)

The E-ISAC establishes situational awareness, incident management, and coordination and communication capabilities with the electricity sector through timely, reliable, and secure information exchange. The E-ISAC shares critical information with electric industry participants regarding infrastructure protection. The goal is to promptly disseminate threat indications, analyses, and warnings and issue alerts to assist electricity sector participants in taking protective action. In addition to its information sharing and coordination roles, the E-ISAC's other responsibilities include analyzing event data, working with the ISACs for other critical infrastructure sectors to exchange information and assistance, performing cyber risk assessments, and participating in critical infrastructure exercises and industry outreach.

E-ISAC seeks to establish situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely information sharing. The E-ISAC works with DOE and the Electricity Sector Coordinating Council (ESCC) to share critical information with the electricity sector, enhancing its ability to "prepare for and respond to cyber and physical threats, vulnerabilities and incidents." The Electricity Sector Information Sharing and Analysis Center, which was established in 1998 under Presidential Decision Directive 63 (President Bill Clinton), called for the establishment of an ISAC for each of the eight infrastructure industries deemed critical to our national economy and public well-being. NERC members who are "registered entities" can report information regarding cyber incidents to ES-ISAC via a secure Internet exchange, and also receive information on threats.

Center for Internet Security (CIS)

Cyber defenders have access to an array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and security checklists, benchmarks, and recommendations. To help understand the threat, threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks are available. Also, there are security requirements, risk management frameworks, compliance regimes, and regulatory mandates. But all of this technology, information, and oversight has become a flood of competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. These are the kinds of issues that led to the CIS Critical Security Controls. They started as a grass-roots activity to cut through the array of inputs and focus on the most fundamental and valuable actions that every enterprise should take. The value is using knowledge and data to prevent, alert, and respond to the attacks that are plaguing utilities and enterprises. Led by the Center for Internet Security (CIS), the CIS Critical Security Controls ("the Controls") have matured with input from an international community of individuals and institutions that: share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action; document stories of adoption and share tools to solve problems; track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions; map the Controls to regulatory and compliance frameworks and bring collective priority and focus to them; share tools, working aids, and translations; and identify common problems (like initial assessment and implementation roadmaps) and solve them as a community instead of alone. See CIS for more details.

The Center for Internet Security's "The CIS Critical Security Controls for Effective Cyber Defense" are a useful set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.[16] A benefit of the Controls is that they prioritize and focus on a smaller number of actions with high pay-off results. The Controls are derived from the most common attack patterns highlighted in threat reports and are vetted across a community of government and industry practitioners to answer the question, "what do we need to do to stop known attacks." The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace.

CIS Critical Security Controls - Version 6.1 (31 August 2016)

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

[16] http://www.cisecurity.org/critical-controls/

U.S. Department of Energy (DOE)[17]

DOE does not have a regulatory role related to electric grid cybersecurity. Instead, the agency supports private industry through technological development and coordination. DOE was designated as the lead agency for the energy sector in the National Infrastructure Protection Plan. DOE's roles in this capacity include providing situational awareness to stakeholders in coordination with DHS and other government agencies; collaborating with DHS and Energy Government Coordinating Council partners to clarify the roles of sector partners and facilitate cooperation with energy stakeholders; and work with DHS and Energy partners to improve coordination of resilience activities.

DOE initiatives include the Cybersecurity for Energy Delivery Systems (CEDS) program, which sponsors research and development to improve cyber defenses, as well as a number of other efforts to help prepare electrical system owners and operators for a potential cyber attack. DOE is home to a number of voluntary initiatives and programs for electric sector cybersecurity, with the Office of Electricity Delivery and Energy Reliability having the lead role.

In 2009, under the FY2010 Energy and Water Appropriations Act (P.L. 111-85), Congress directed DOE to form a national organization to serve as the National Electric Sector Cybersecurity Organization resource that would "institute research, development and deployment priorities, including policies and protocol to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid." DOE selected two organizations to form the National Electric Sector Cybersecurity Organization (NESCO): EnergySec and the Electric Power Research Institute (EPRI). EnergySec provides support for "information sharing, professional development and collaborative programs and projects that improve the cyber security posture of all participating organizations." EPRI serves as the research and analysis resource for NESCO. NESCO's mission is to improve the "cybersecurity posture of the electric sector by establishing a broad-based public-private partnership for collaboration and cooperation" by providing a forum for cybersecurity experts, developers, and systems users.

The Cybersecurity Capability Maturity Model (C2M2) was developed by DOE, the Department of Homeland Security (DHS), and industry as a self-evaluation survey tool for any organization to address cybersecurity vulnerabilities. The C2M2 asks users to assess cybersecurity control implementation across 10 areas of cybersecurity "best practices" based on an evaluation of the maturity of a specific cybersecurity function. The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) goes one step further, specifically tailoring the core C2M2 survey for the electricity subsector with a "maturity model, an evaluation tool, and DOE facilitated self-evaluations." Additionally, in 2006, DOE released a report titled Roadmap to Secure Control Systems in the Energy Sector. It outlined a strategic framework to be developed by industry, vendors, academia and government stakeholders to "design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber-incident while sustaining critical functions." The plan called for a 10-year implementation timeline focusing on barriers and recommended strategies for achieving effective grid cybersecurity. A five-year update released in 2011 highlighted what had been achieved to date, discussing ongoing efforts with respect to short- to long-term goals.

U.S. Department of Homeland Security (DHS)

DHS has a broad mission to make the United States safe and resilient against terrorism and other potential threats. The cyber and physical security of the grid are encompassed in this mission, and DHS has several initiatives in pursuit of these goals. The DHS National Protection and Programs Directorate (NPPD) coordinates national efforts to protect critical infrastructure, working with partners "at all levels of government, and from the private and non-profit sectors" to share information to make critical infrastructure more secure. Under NPPD are several offices focused on cybersecurity, critical infrastructure protection, and resiliency. NPPD is the home of the National Cybersecurity and Communications Integration Center (NCCIC, is focused on "cyber situational awareness, incident response, and management." NCCIC acts as an information sharing forum for the public and private to

[17] A substantial portion of material on DOE, DHS, NIST, ESCC, and EEI came from Bipartisan Policy Center Report, "Cybersecurity and the North American Grid," February 2014. See the organizations' web sites for additional current details.

improve understanding of cybersecurity and communications vulnerabilities and incidents, and mitigation and recovery from cyber events. NCCIC's mission is to reduce the likelihood and severity of incidents that may "significantly compromise the security and resilience of the Nation's critical information technology and communications networks."

Two critical branches of NCCIC with functions important to electric grid cybersecurity are the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

ICS-CERT reduces risk to the nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for Critical Infrastructure and Key Resources stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies. US-CERT developed the Einstein 2 intrusion detection system used by the National Cybersecurity Protection System (NCPS). NCPS intrusion detection capabilities alert DHS to the presence of malicious or potentially harmful computer network activity transiting to and from participating in federal executive branch civilian agencies' information technology networks. This capability is deployed via EINSTEIN 2 and provides for improved detection and notification capabilities to provide near real time response to cyber threats. ICS-CERT coordinates responses to control systems-related security incidents and facilitates information sharing among federal, state, and local agencies and organizations; the intelligence community; and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

The DHS Science and Technology Directorate (S&T) was created to provide science and technology in support of DHS's mission. Since DHS assists in efforts for the security and resiliency of the grid, the Smart Grid with characteristics of self-healing from power disturbance events, and operating resiliently against physical and cyber threats is of particular interest. S&T also has a Cyber Security Division whose mission is to enhance the security and resilience of the nation's critical information infrastructure and the Internet by

- Developing and delivering new technologies, tools and techniques to enable the United States to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks;
- Conducting and supporting technology transition; and
- Leading and coordinating cybersecurity research and development for department customers, and with government agencies, the private sector and international partners.

Since recovery from cyberattacks is seen as a part of S&T's resiliency focus, S&T is working on several electric power sector specific initiatives. These include the Resilient Electric Grid (an effort to "keep the lights on" in the event of a power outage by enabling distribution level power substations to share power with one another), and the Recovery Transformer (a program developing a prototype large power transformer to enable a quicker recovery [i.e., within days instead of months or years] from an event which might damage key transformers). S&T is currently managing an effort to assess the state of the Smart Grid concept, as well as specific technologies needed to achieve goals of ensuring Smart Grid security and resiliency.

National Institute of Standards and Technology (NIST)

The Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140) defined attributes of a Smart Grid and plans for its development, and also gave NIST the role of coordinating the development of a framework to enable the development of the Smart Grid in a safe and secure manner. Because cybersecurity threats were perceived as "diverse and evolving," NIST advocated a defense-in-depth strategy with multiple levels of security and asserted no single security measure could counter all types of threats. The key to NIST's suggested approach is the determination of risk (i.e., the potential for an

unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences) as quantified by the threat (e.g., event, actor or action with potential to do harm), the vulnerability (e.g., weakness in the system), and the consequences (e.g., physical impacts) to the system.

NIST published its Guidelines for Smart Grid Cybersecurity as a comprehensive, voluntary framework for organizations to use in developing effective cybersecurity strategies "tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities." According to NIST, deliberate attacks are not the only threat to Smart Grid cybersecurity. Smart grid cybersecurity must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. NIST established the Smart Grid Interoperability guidelines with a primary goal of developing a cybersecurity risk management strategy to enable secure "interoperability" of technologies across different Smart Grid domains and components. NIST was asked in 2013 by Presidential Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," to lead the development of a "Cybersecurity Framework" to reduce cyber risks. The framework was based on industry methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks, incorporating "voluntary consensus standards and industry best practices to the fullest extent possible." The first version of the Framework was released on February 12, 2014. Sector-specific federal agencies (such as DOE) are to report annually to the President on the extent to which owners and operators of critical infrastructure at greatest risk are participating in the program. NIST also hosts the National Cybersecurity Center of Excellence, which is focused on getting better adoption of secure, commercially available cybersecurity technologies by both the public and private sectors.

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems..." To carry out its EISA-assigned responsibilities, NIST devised a three-phase plan to rapidly establish an initial set of standards, while providing a robust process for continued development and implementation of standards as needs and opportunities arise and as technology advances. The Smart Grid Interoperability Panel (SGIP) was born from that plan and in January 2013, fully transitioned to a private/public partnership funded by industry stakeholders in cooperation with the federal government.

Electricity Sub-Sector Coordinating Council (ESCC)

ESCC is the principal liaison between the federal government and the electric power sector. It represents the electricity sub-sector (as part of the Energy Critical Infrastructure sector) under DHS's National Infrastructure Protection Plan (NIPP). The ESCC draws its membership from all segments of the electric utility industry, and is led by three chief executive officers—one each from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association. Among its activities, the ESCC coordinates industry and government efforts on grid security, guides infrastructure investments and R&D for critical infrastructure protection, seeks to improve threat information sharing and processes with public and private sector stakeholders, and coordinates cross sector activities with other critical infrastructure sectors. A Senior Executive Working Group (SEWG) supports the mission and activities of the ESCC, creating ad hoc "sub teams" to address goals identified by utility and government executives.

The Edison Electric Institute (EEI)

EEI is the trade association for investor-owned electric utilities that has been involved with the formation of industry partnerships on cybersecurity issues with a number of federal agencies. Information sharing between public and private entities is an issue the industry considers critical in protecting the grid against cyber-threats. Industry is involved in several information sharing efforts including the E-ISAC, ESSC, and NCCIC.

International Electrotechnical Commission (IEC)

Important international standards are provided by the International Electrotechnical Commission (IEC), including IEC62443 Standard. IEC's Technical Committee develops standards for information exchange for power systems. The International Electrotechnical Commission's 2016 technical report on "Resilience and security recommendations for power systems with distributed energy resources

(DER) cyber-physical systems" (IEC TR 62351-12:2016) provides cyber security recommendations and engineering and operational strategies for improving the resilience of power systems with interconnected DER systems. It covers resilience requirements for the many different stakeholders of these dispersed cyber-physical generation and storage devices, with the goal of enhancing the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems. It addresses resilience and cyber security issues for cyber-physical DER systems interconnected with the power grid. The IEC technical report builds on the concepts and the hierarchical architecture described in the Smart Grid Interoperability Panel's Distributed Renewables, Generation and Storage Subgroup B White Paper "Categorizing Use Cases in Hierarchical DER Systems"(dated *01-14-2014)*, and discussed in the IEC 61850 "Information Model Concepts and Updates for Distributed Energy Resources (DER) Use Cases and Functions", a white paper developed by the Smart Grid Interoperability Panel (October 2015). (IEC 2016) Using and enhancing these standards over the next decade provide a technical basis for international cyber security regulations regarding utilities.

Government and Industry Cooperation on Grid Cybersecurity

Cooperation between the federal government and the electric power sector now extends beyond mandatory and enforceable industry standards for the bulk electric system. However, such cooperation has not always been typical. While a number of voluntary structures now exist for information sharing and cybersecurity strategies, the degree of adoption by electric utilities and the overall effectiveness of these programs is unknown.

UCA International Users Group

UCA International Users Group is a not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The Users Group does not write standards, however works closely with those bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange). The UCAIug as well as its member groups (CIMug, Open Smart Grid, and IEC61850) draws its membership from utility user and supplier companies. The mission of the UCA International Users Group is to enable integration through the deployment of open standards by providing a forum in which the various stakeholders in the energy and utility industry can work cooperatively together as members of a common organization to:

- Influence, select, and/or endorse open and public standards appropriate to the energy and utility market based upon the needs of the membership.
- Specify, develop and/or accredit product/system-testing programs that facilitate the field interoperability of products and systems based upon these standards.
- Implement educational and promotional activities that increase awareness and deployment of these standards in the energy and utility industry.
- Influence and promote the adoption of standards and technologies specific to the ever-increasing Smart Grid initiatives worldwide.

European Commission

In July 2016, the European Commission issued a communication on "strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry.[18] The European Commission also created the "Energy Expert Cyber Security Platform" (EECSP) with the aim of providing guidance to the Commission on policy and regulatory direction EU-wide. The first European legislation on cybersecurity, the Network and Information Security (NIS) Directive, was issued in July 2016 and entered into force August 2016. The directive provides legal measures to increase the overall level of cybersecurity in the EU by increasing cybersecurity capabilities in member states, enhancing cooperation on cybersecurity among member states, and requiring operators of essential services in the energy sector to take appropriate security measures and report incidents to national authorities.

[18] The European Union (European Parliament and the Council) Directive 2016/1148, concerning measures for a high common level of security of network and information systems across the Union, was issued on July 6, 2016.

Once implemented, European consumers, governments, and businesses will be able to rely on more secure digital networks and infrastructure to reliably provide essential electricity services. However, significant coordination on the part of member states is required to reach similar levels of cybersecurity across all of the European Union. Moreover, although the NIS is a promising first step, more explicit cybersecurity regulations and best practices will need to be implemented in Europe.

The European Commission NIS directive:

- Requires member states to adopt a national strategy for NIS security
- Creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
- Improves cooperation and trust between member states by the creation of a computer security incident response teams (CSIRT) network
- Establishes security and notification requirements for operators of essential services
- Lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

United Kingdom

In the UK, Government advice such as '10 steps to Cyber Security' are intended to provide a baseline level of cyber security for companies. Ofgem's regulatory role is to ensure that the regulatory framework allows companies to put in place measures if, and as, specified by government. Ofgem works closely with government, industry and other national regulatory authorities to understand the cyber security threat and mitigating actions required.

Appendix D: Resiliency to Achieve High Reliability[19]

Electricity service reliability is a key aspect of a properly functioning power system. Achieving high reliability requires focus on all aspects of assuring electricity delivery, and having the resiliency to quickly respond to cyber attacks or physical failures. In order to get reliability of 99.99% (outage of less than 1 hour per year), properly operating cyber systems and physical components and systems need to be effectively maintained and protected.

The digital fabric that integrates the Electric Power grid provides opportunities for improving reliability and reducing costs. That digital interconnection is key to providing flexibility to utilize intermittent renewable energy resources such as wind and solar. The digital "smart grid" utilizes technologies being developed by the information technology and data communications industries and will evolve as more advanced digital systems are employed. However, the interconnectedness of these systems also introduces many more vectors for potential cyber penetrations, and increases the vulnerabilities of the Utilities of the Future-- unless robust and effective cybersecurity preventive and protective measures are taken. In addition, with the gathering and consolidation of data, there are the issues of information privacy for electric utilities and other interconnected information technology systems.

In military parlance, mission assurance is the focus on assuring that the endeavor (or military mission) can be successfully carried out, and that all the key supporting systems, people, and equipment are available and effective, even if the assumptions and events turn out to be different than planned. The analogy for the electric utilities is that mission assurance is the focus on delivering reliable electricity, even if the assumptions of stable equipment and no external or internal attacks turn out to be different than planned. Mission assurance for electric utilities requires focus on all aspects of electrical generation, including impact of multiple generators and distributed energy resources not in their direct control.

No fully secure network protected from all cyber-attacks or physical failures is possible, so must assume penetration and failures. Good resiliency requires dealing with compromised systems and having disaster recovery plans in place. To provide resiliency, vulnerabilities need to be assessed and reduced, attacks prevented when possible, effective speedy response when attack occurs, and a thoughtful plan to recover and restore operations.

In a study for the National Association of Regulatory Utility Commissioners, (Stockton, 2014) utilities were recommended to consider extraordinary and hazardous catastrophes utterly unlike the "blue sky" days (clear sky with no storms) during which utilities typically operate. The resilience challenges posed by "black sky" days (dark stormy weather) go above and beyond those posed by Superstorm Sandy in the United States, the U.S. Derecho Storms of 2012, or other recent Major Outage Events. Building resilience against large-scale hurricane events is vital, given the increasing frequency and severity of such storms. These extraordinary and hazardous events will pose special risks to the resilience of electric utilities. Metrics for resilience should supplement, not replace, the reliability metrics that have been refined over many decades. Loss of Load Expectation (LOLE) or Loss of Load Probability (LOLP) analysis is performed on a system to determine the amount of capacity that needs to be installed to meet the desired reliability target, commonly expressed as an expected value in number of hours or days in a year.[20] Expected Energy Not Served (EENS) is the expected number of megawatt hours per year that a system must curtail due to inadequate generation.

NARUC's Resilience in Regulated Utilities (hereinafter referred to as the NARUC Resilience Report) notes that resilience has been defined in a variety of ways. Many definitions, however, are similar to that provided by Presidential Policy Directive 21, which defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring incidents." Measures of electric outage frequency, such as the System Average Interruption Frequency

[19] Information in this section comes from many sources including Stockton. 2016.

[20] http://www.nerc.com/files/ivgtf1-2.pdf

Index (SAIFI), can help commissioners assess the ability of utilities to "withstand" incidents without incurring a loss of service. Measures of outage duration, such as the System Average Interruption Duration Index (SAIDI), can help assess the ability of utilities to "recover rapidly" from disruptions. Reducing the frequency and duration of outages will remain an essential goal for public utility commissioners, and reliability metrics provide the indispensable foundation on which to build a framework to assess resilience. Regardless of definition, however, collecting reliability data on Major Outage Events can allow commissioners to more clearly assess a key focus of resilience – that is, how quickly utilities can "bounce back" or recover after disasters and restore service when a crisis occurs.

A large-scale cyber attack on the electric grid would present governance and coordination challenges in addition to difficult technical and logistical challenges. Not only would a successful attack require cyber-specific responses, such as the removal of malware, it would likely also require more traditional disaster response operations to deal with resulting threats to public health and safety. Efficient and ongoing communication will clearly be critical, along with effective coordination, a clear chain-of-command, and the ability to adapt quickly as new information emerges. While Executive Order 13636 has helped clarify cybersecurity roles and responsibilities within the federal government, questions remain concerning the specific responsibilities of different agencies and chain-of-command in the event of an attack. The National Response Framework (NRF), the third addition of which was updated in 2016, provides context for how the whole community works together and how response efforts relate to other parts of national preparedness. It was designed to address physical and other impacts from "traditional" disasters (such as a hurricanes or floods). (Bipartisan 2014) In July 2016, President Obama issued Presidential Policy Directive 41 (PPD-41): United States Cyber Incident Coordination. The directive called for a National Cyber Incident Response Plan (NCIRP) that defines a nationwide approach to cyber incidents and outlines the roles of both federal and non-federal entities. It also outlines how the U.S. government prepares for, responds to, and recovers from significant cyber incidents. It responds to calls from the private sector to provide clarity and guidance about the Federal Government's roles and responsibilities, including an answer to the question, "who do I call to report cyber incidents and get help?"[21]

Resilience against cascading blackouts and terrorist acts requires advance planning. Electric utilities, working in consortiums, may consider stockpiling old transformers and other devices in case needed for response (instead of scrapping).

Many of the most significant threats of "black sky" events (really bad events, in contrast to "blue sky" or smoothly operating normal events) either rarely happen, or have yet to occur (as in the case of large scale, coordinated cyber attacks on industrial control systems and control center data essential for operating the power grid). If these events do occur, however, their effects would be catastrophic. Therefore, Public Utility Commissions need to build an enterprise risk management system to account for these bad events. Under a risk management system (where risk is assessed in terms of threat, vulnerability, and consequence), the starting point for commissioners and their staffs should be to develop an assessment of the threats that their utilities are most likely to confront. There are a number of possible sources of threat data to build such an assessment. State Energy Assurance Plans -- developed by the State Energy Offices under the umbrella of the National Association of State Energy Officials (NASEO) in partnership with the US Department of Energy (DOE) -- often include data on significant State-specific hazards. In each of the ten Federal Emergency Management (FEMA) regions, FEMA Regional Coordinators and their State and local partners are examining the most likely catastrophic threats to their areas, which will then serve as a basis for catastrophic response planning (including preparedness for the impact of extended power outages on public health and safety). State National Guard Joint Force Headquarters assesses natural and manmade hazards in each State. The Department of Homeland Security supports Fusion Centers in many States that track threat data. The Federal Bureau of Investigations Joint 42 Central United States Earthquake Consortium's Capstone Exercise, Private Sector Workshop,[22] and Terrorism Task Forces (JTTFs) may also be able to provide helpful data on manmade threats. While necessary, however, these assessments of likely threats will

[21] www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment

[22] www.cusec.org/plans-a-programs/capstone14/176

fall short of providing reliable predictions of event probability. A risk management process would involve three primary components:

1. Comprehensive region-wide assessment of risks to the critical assets identified and their interdependencies, including a detailed assessment of current protection measures and response and recovery capabilities;
2. Evaluation of risk mitigation solutions, including cost-benefit analysis to compare the life-cycle cost of identified solutions with their risk reduction potential; and
3. Time-based tracking and comparison of region-wide risk, including an evaluation of changes in criticality, threat, and preparedness that would alter the overall risk profile of the utilities within each region

Regulatory commissions may want to explore preparedness against the worst effects of major disruptions, focused on the most extreme, high consequence hazards. Questions to consider:

- How do companies integrate resilience into enterprise risk management structures?
- What corporate structures and governance drive performance for resilience?
- Do you conduct exercises to prepare for severe, non-traditional hazards? How have you adjusted your restoration plans and crew training for severe events?
- Which catastrophic threats does your company see as most probable? What "keeps you up at night?"
- What is the minimum power delivery level that should be maintained to avoid an irreversible loss of critical systems (water, health, finance, food, etc.)?
- How could power utilities perform operations to allow a graceful degradation of power services?
- Have utilities had discussions with State and local emergency managers, National Guard leaders, or other officials within their region on the probability of (and preparedness against) catastrophic hazards, and the challenges these hazards create for power restoration?
- Have utilities had discussions with key stakeholders or other critical sectors on the consequence for those sectors of a long-term power outage?
- In a severe event (such as an earthquake), natural gas pipelines and other energy infrastructure systems essential for power generation may not only be disrupted by electricity outages, but may themselves be damaged. How to account for these risks in your restoration planning?
- In a similar way, the infrastructure that your utility crews need to restore power may be disrupted. Communications systems are a prime example. What measures are you taking to address these challenges for resilience?
- Recognizing that information sharing is useful for improving resilience, but paradoxically may raise system vulnerabilities, how much information should be shared and how widely?

Commissioners already have a set of highly effective assessment tools, including the Interruption Cost Estimate (ICE) Calculator and the Argonne RMI (Resilience Measure Index) calculator, to help them assess the costs and benefits of proposed investments in resilience. Adapting or supplementing these tools to help commissioners perform cost-benefit analysis for resilience investments. Minimizing the risks of outages in catastrophic events is important, but commissioners have incentive to develop and improve tools that help them avoid low-payoff investments.

DOE could fund efforts to understand systemic cyber risks, including risks involving interdependencies and the spillover of consequences from one firm or jurisdiction to another. DOE could fund research to help regulators better evaluate the potential impacts of cyber attacks and weigh the benefits of cybersecurity investments. DOE should work with industry and state regulators to develop metrics for evaluating utility investments in cybersecurity. These metrics could then be used in cost-recovery determinations. (Bipartisan 2014)

Robust mutual assistance mechanisms can be used. For instance, the Regional Mutual Assistance Group provides a system by which utilities can support each other with utility crews and other assets. Many municipal power systems and electric cooperatives also have strong mutual support arrangements. The Spare Transformer Equipment Program (STEP) and other mechanisms to share critical grid components between U.S. utilities further strengthen their ability to speed power restoration in large-scale power interruptions.

REFERENCES

Chapter 1

Campbell, R.J. 2015. Cybersecurity Issues for the Bulk Power System. Washington DC: Congressional Research Service. R43989; 7-5700. June 10, 2015. www.fas.org/sgp/crs/misc/R43989.pdf.

Bipartisan Policy Center, 2014. "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address the Evolving Threat." February 2014

EIA. 2016. "How many smart meters are installed in the United States, and who has them?" US Energy Informaiton Adminstration Frequently Asked Questions. www.eia.gov/tools/faqs/faq.cfm?id=108&t=3

Electricity-ISAC and SANS Industrial Control Systems. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Electricity-Information Sharing and Analysis Center. ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Chapter 2

Campbell, R.J. 2015. Cyberecurity Issues for the Bulk Power System. Washington DC: Congressional Research Service. R43989; 7-5700. June 10, 2015. www.fas.org/sgp/crs/misc/R43989.pdf.

Choucri, N., S. Madnick, and P. Koepke. 2016. "Institutions for Cyber Security: International Responses and Data Sharing Initiatives." MIT Sloan School Cybersecurity Interdisciplinary Systems Laboratory. August 2016. web.mit.edu/smadnick/www/wp/2016-10.pdf.

Cleveland, F. and A. Lee. 2013. "Cyber Security for DER Systems." National Electric Sector Cybersecurity Organization Resource. Electric Power Research Institute (EPRI). July 2013. smartgrid.epri.com/doc/der-rpt-07-25-13.pdf.

Electricity-ISAC and SANS Industrial Control Systems. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Electricity-Information Sharing and Analysis Center. ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Hampson A., T. Bourgeois, G. Dillingham, and I. Panzarella. 2013. *Combined Heat and Power: Enabling Resilient Energy Infrastructure for Critical Facilities.* ICF International Report for Oak Ridge National Laboratory. March 2013.

IEC. 2016. "Resilience and Security Recommendations for Power Systems with Distributed Energy Resources (DER) Cyber-physical Systems." IEC TR 62351-12:2016. International Electrotechnical Commission. April 2016.

Lloyd's. 2011. "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid." Lloyds' Emerging Risk Report. www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

Marnay C., H. Aki, K. Hirose, A. Kwasinski, S. Ogura, and T. Shinji. 2015. "Japan's Pivot to Resilience: How the Microgrid Fared after 2011 Earthquake." *IEEE Power & Energy Magazine* 13(3): 44-57. May 2015.

MIT. 2011. *The Future of the Electric Grid*. Chapter 9. Cambridge, MA: Massachusetts Institute of Technology. December 2011.

NIST. 2014a. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. National Institute of Standards and Technology. February 12, 2014. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST. 2014b. “Interagency Report on Guidelines for Smart Grid Cybersecurity.” NISTIR 7628: Volumes 1-3. National Institute of Standards and Technology. September 2014.

Nourian, A. and S. Madnick. 2015. "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems: Applied to Stuxnet." To appear in IEEE Transactions on Dependable and Secure Computing. MIT Sloan School Cybersecurity Interdisciplinary Systems Laboratory. December 2015. web.mit.edu/smadnick/www/wp/2015-07.pdf.

NRC. 2012. “Terrorism and the Electric Power Delivery System." In Mitigating the Impact of Attacks on the Power System. National Research Council. Washington, DC: The National Academies Press. doi:10.17226/12050. www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

Rogers, M.S. 2016. “Statement before the Senate Armed Services Committee.” April 5, 2016. www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

Scottmadden Management Consultants. 2015. *Energy Industry Cybersecurity Report*. July 2015.

Shelar, D. and S. Amin. 2016. “Security Assessment of Electricity Distribution Networks under DER Node Compromises.” IEEE Transactions on Control of Network Systems.

Smith, E., et al. 2016. “Going Beyond Cybersecurity Compliance.” *IEEE Power and Energy Magazine*. September/October 2016.

Stockton, P. 2016. “Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System.” The Johns Hopkins University Applied Physics Laboratory. NSAD-R-15-075.

Ton D.T. and M.A. Smith. 2012. “The U.S. Department of Energy’s Microgrid Initiative.” *The Electricity Journal* 25(8): 84-94. October 2012.

Chapter 3

European Union. 2016a. Directive (EU) 2016/1148: Concerning measures for a high common level of security of networks and information systems across the Union. European Union, Brussels, Belgium: July 6, 2016.

European Union. 2016b. Regulation (EO) 2016/679: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union, Brussels Belgium: April 27, 2016.

NERC. 2016. Critical Infrastructure Protection Standards. North American Electric Reliability Corporation, Washington, DC, 2016.

Chapter 4 and 5

none

Appendicies

Bipartisan Policy Center, 2014. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address the Evolving Threat.” February 2014

Black & Veatch, 2014. “Strategic Direction: U.S. Electric Industry,” 2014.

Campbell, R.J. 2015. Cybersecurity Issues for the Bulk Power System. Washington DC: Congressional Research Service. R43989; 7-5700. June 10, 2015. www.fas.org/sgp/crs/misc/R43989.pdf.

CSIS 2016. Center for Internet Security, “The CIS Critical Security Controls for Effective Cyber Defense,” 2016

IEC. 2016. “Resilience and Security Recommendations for Power Systems with Distributed Energy Resources (DER) Cyber-physical Systems.” IEC TR 62351-12:2016. International Electrotechnical Commission. April 2016.

MIT. 2011. *The Future of the Electric Grid*. Chapter 9. Cambridge, MA: Massachusetts Institute of Technology. December 2011.

NIST 2014. NIST 2014. National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." 2014.

Stockton, Dr. Paul. 2014. Resilience for Black Sky Days Supplementing Reliability Metrics for Extraordinary and Hazardous Events, The National Association of Regulatory Utility Commissioners, , February 2014

Stockton, Paul. 2016. Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System, Johns Hopkins Applied Physics Laboratory, 2016