California Public Utilities Commission

Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission

GRID PLANNING AND RELIABILITY POLICY PAPER

Elizaveta Malashenko
ENERGY DIVISION

Chris Villarreal
POLICY AND PLANNING DIVISION

J. David Erickson
ENERGY DIVISION

September 19, 2012

The views presented in this paper are those of staff and do not necessarily represent the views of the five member California Public Utilities Commission. This paper is intended to initiate a dialog on the topics discussed and any recommendations are preliminary. Staff may revise this paper based on further discussion and comments received.

Executive Summary

With grid modernization or "Smart Grid" efforts underway, cybersecurity is being recognized as an increasingly important factor in ensuring resiliency, reliability and safety of the electrical system. In recent years, cybersecurity has become a top national security issue and, as a result, safeguarding the cybersecurity of the electrical grid is increasingly recognized as vital. Cybersecurity is critical for both guaranteeing privacy of energy consumers and for capturing grid modernization benefits. As the electrical grid is modernized through deployment of "smart" devices, communication networks and control systems, cybersecurity has to become a foundational consideration.

From a regulatory perspective, grid cybersecurity has been addressed most actively at the Federal level. Cybersecurity for the grid is handled through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. These requirements provide a framework for protecting the reliability of the North American utility industry's bulk electric system by identifying and protecting critical cyber-assets whose security directly affects utility operations.

However, the NERC-CIP framework has important limitations. First, NERC-CIP primarily covers only generation and transmission assets that qualify as "critical assets" or "critical cyber-assets." With grid modernization, this identification is becoming increasingly problematic as many assets, such as advanced meters, do not fall under NERC-CIP but can have a major impact on grid reliability, safety and customer privacy. Estimates range from 80 percent to over 90 percent of grid assets are outside NERC-CIP's scope today[1]. Second, NERC-CIP is primarily a compliance-based policy. Compliance is an important component of addressing cybersecurity, but it is not enough to ensure that the rapidly evolving risks are adequately considered and acted upon effectively.

In addition to NERC-CIP, there are a number of cybersecurity standards and requirements from various entities, but individual utilities and the technology providers often lack a business case to justify spending on cybersecurity beyond minimal compliance. A broader risk management-based approach is needed to move beyond minimal compliance and mitigate cybersecurity risks as they arise.

State regulators have not traditionally played a large role in cybersecurity. However, this is beginning to change with the recognition that Federal compliance-based models may not be sufficient to ensure grid resiliency, reliability and safety, as well as customer data privacy. With grid modernization on

[1] Ernie Hayden, Managing Principal, Energy Security, Verizon Energy & Utility Practice, provided an estimate of 97 percent. This number is not specific to California utilities. Transmission facilities owned/operated by California utilities represent about 10 percent of total transmission and distribution conductor miles, based on figures obtained from utility financial reports. Transmission-only substations and combined transmission and distribution switching substations are about 15 percent of the total number of substations in California. These figures put the total IOU-operated distribution level infrastructure under the purview of the CPUC at slightly less than 90 percent of total utility T&D assets in California.

the way, there is an important role that State regulators need to step into, as much of this new infrastructure will be located on the distribution grid, which is currently outside of NERC authority. There is also a possibility that the Federal government could preemptively move to regulate in this area if there is no action at the State level.

The California Public Utilities Commission (CPUC) is committed to the importance of risk management in reliability and safety. Following the rupture of a Pacific Gas and Electric (PG&E) pipeline in San Bruno, California, in 2010, the CPUC has been working to implement recommendations made by an Independent Review Panel and the National Transportation Safety Board. As part of that implementation, the CPUC has recognized that explicit safety and security risk assessment that includes cybersecurity should become the cornerstone of how the CPUC approaches reliability and safety, particularly through the General Rate Case (GRC) process. The CPUC could also apply a similar risk assessment framework to cybersecurity for the electric industry. The CPUC has also established privacy rules for customer data and has required utilities to report on cybersecurity activities in their Smart Grid Deployment Plans.

The purpose of this paper is to examine how the CPUC and other State regulators can further address cybersecurity as it relates to grid resiliency, reliability and safety. In particular, this paper recommends that the CPUC opens an Order Instituting Rulemaking (OIR) to further investigate appropriate cybersecurity policies.

Key Takeaways

1. As the State moves forward with grid modernization, utilities must design and implement both cyber and physical security policies that protect public safety, enhance the reliability and resiliency of the grid and protect customer privacy from cyber threats, and do so cost-effectively.
2. While there are many cybersecurity related activities at the Federal level, 80-90 percent or more of the electric infrastructure currently does not fall under any required standards and cybersecurity practices of the utilities are not monitored.
3. State regulators have not traditionally played a large role in cybersecurity, but that is starting to change with grid modernization efforts that are underway. Absent comprehensive action at the State level, the Federal government may attempt to preemptively expand its regulation to cover utility cybersecurity practices
4. There are many examples of cybersecurity events that have already taken place, such as Stuxnet, Aurora, a number of Smart Meter hacks, RuggedCom and others.
5. It is important for State regulators to understand the nature of the cyber-threats, vulnerabilities, and overall risks in cyberspace faced by the utilities, and to understand how the utilities are assessing these risks. It is important for regulators to have a clearly defined role in supporting the adherence to overall cybersecurity standards and safety.

6. There are a number of cybersecurity standards, but individual utilities and their technology providers often lack a business case to spend on cybersecurity beyond minimal compliance. There is no such thing as a 100 percent secure system. Utilities and State regulators should explore a risk management-based approach to cyber-events in order to maximize responsiveness to changing threats and should also ensure that the system is designed to be resilient.
7. Many other State regulators in addition to CPUC have started developing cybersecurity policies, including public utility commissions in Michigan, Pennsylvania and Texas. Additionally, the National Association of Regulatory Utility Commissioners (NARUC) passed a resolution in 2010 that encouraged State regulators to open a dialogue with their regulated utilities to promote policies that ensure implementation of cost-effective protection and preparedness measures to deter, detect, and respond to cybersecurity threats.
8. Ensuring security of the electric grid infrastructure will include the regulators, utilities and technology providers working together to address the cybersecurity risks and vulnerabilities.

Recommendations

- The CPUC should open an Order Instituting Rulemaking (OIR) to explore cybersecurity best practices and develop a cybersecurity approach for the investor-owned utilities in California.
- Potential decisions for the CPUC related to regulatory strategy for cybersecurity include:
    - What actions can CPUC take to address cybersecurity to ensure public safety and reliability?
    - What is the CPUC position on the role of the NERC-CIP cybersecurity requirements for the distribution grid?
    - What are the proper regulatory mechanisms to ensure cybersecurity, including a combination of compliance-based and risk assessment-based approaches?
    - How can CPUC ensure that the utilities and their technology providers are properly incentivized to adequately address cybersecurity?
    - What requirements should be developed to ensure that the electric system is designed to be resilient to cyber-events?
    - What are the metrics that can be used to track effectiveness of cybersecurity policies and investments?
    - How do confidentiality rules apply to cybersecurity related reporting?
- The CPUC should consider safe harbor protections to encourage utilities to share information regarding security breaches and attacks.
- CPUC should evaluate the skill-sets and resources needed for CPUC Staff to adequately address cybersecurity.

Table of Contents

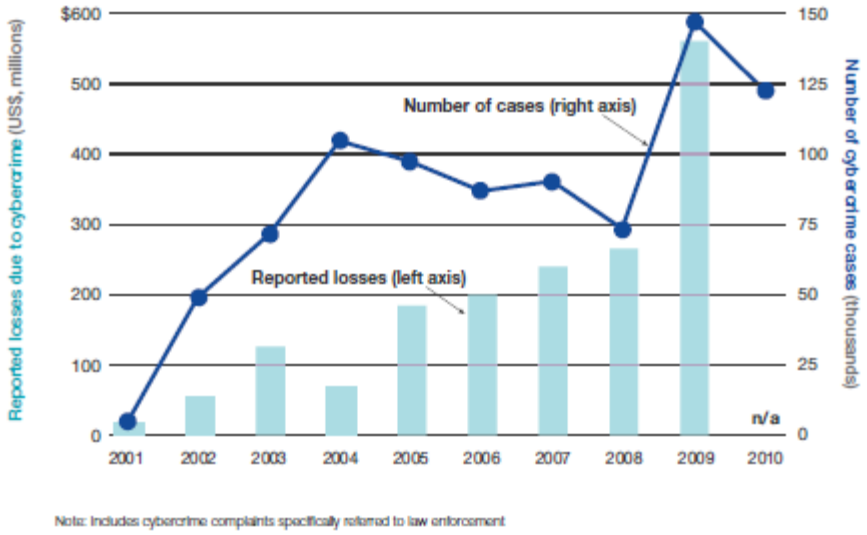
Executive Summary iii
Key Takeaways iv
Recommendations v
1 The Importance of Cybersecurity in the Energy Industry 1
1.1 Utility Operations Combine Cyber and Physical Aspects 2
1.2 Utility Systems and Cybersecurity 2
1.3 Cyber-Attacks and Risk 2
1.4 Potential Impact of a Cyber-Attack on a Utility System 4
1.5 Examples of Cybersecurity Events in the Energy Industry 5
1.5.1 Stuxnet 5
1.5.2 Aurora 5
1.5.3 Smart Meter Hack 5
1.5.4 RuggedCom 5
1.5.5 Shodan 5
1.5.6 San Onofre 6
2 Government's Role in Cybersecurity 6
2.1 Cybersecurity Planning 7
2.2 Legislative Action in Cybersecurity 7
2.3 Federal Regulatory Bodies and Standards 8
2.3.1 NERC Critical Infrastructure Protection Overview 8
2.3.2 Limitations of NERC-CIP 9
2.3.3 NRC 10
2.3.4 NIST and Smart Grid 10
2.3.5 NISTIR 7628 11
2.3.6 DOE Risk Management Process 11
2.3.7 Risk Management Maturity Model 12
2.3.8 Other Voluntary Standards 12
3 Key Cybersecurity Challenges for State Regulators 12
3.1 Constantly Changing Threats and Vulnerabilities 13
3.2 Instrument Control and Embedded Systems Challenges 13
3.3 Greater Organizational Integration 13

3.4 Voluntary versus Mandatory Security Measures 14
3.5 Risk-based Approach to Cybersecurity 15
3.6 Including Cybersecurity in Grid Modernization Design Process 15
3.7 The Need for Information Sharing 16
4 Emerging Role of State Regulation in Cybersecurity 17
4.1 Evolving Role of State Regulators 17
4.2 Example of State Regulatory Action: California 18
4.3 Example of State Regulatory Action: Michigan 19
4.4 Example of State Regulatory Action: Pennsylvania 19
4.5 Example of State Regulatory Action: Texas 20
5 Proposed Next Steps for the CPUC 21
5.1 Key Cybersecurity Questions for the CPUC 21
5.2 Consideration of Cybersecurity as an Aspect of Grid Safety and Reliability 21
5.3 Options for CPUC Action 22
6 Conclusion 23

1 The Importance of Cybersecurity in the Energy Industry

As a society, we are increasingly dependent on digital technologies and, as a result, cybersecurity[2] has become a prominent issue, with companies across all industries taking steps to protect themselves from intentional and unintentional breaches. The economic impact of cyber-attacks on businesses has grown to over $100 billion annually[3] and security breaches are on the increase, increasing by over 100 times since 2001. Attacks on Federal agencies increased 206 percent between 2006 and 2008.[4]

Figure 1: Cost and Incidence of Cyber-crime in the US



Source: PwC, 2011

As the grid is modernized, the "attack surface" of utility operations is significantly increased and can be expected to be subjected to a level of attempts to breach security similar to that seen in other industries. Ensuring cybersecurity of the utility infrastructure will require a significant investment, with cumulative utility Smart Grid cybersecurity related investments for both installed and new infrastructure in the next six years estimated to total $14 billion nationwide.[5]

[2] For the purpose of this paper, the term cybersecurity describes the systems and methods used to defend, deter, isolate, and detect unwanted intrusions into computer-based operations.

[3] "Cyber Crime: Protecting Against the Growing Threat," Price Waterhouse Coopers, November 2011.

4 "Cyber Threats and Vulnerabilities Place Federal Systems at Risk," General Accounting Office, May 5, 2009.

5 "Smart Grid Cyber Security," Pike Research, October 17, 2011.

1.1 Utility Operations Combine Cyber and Physical Aspects

With modern technologies being deployed throughout the utility industry, it is becoming increasingly difficult to separate the "cyber" sphere from the "physical" asset sphere. Traditional utility assets, such as transformers, switches and reclosers, are being automated and connected with utility operations through two-way digital communication networks. While this technology provides benefits to the utilities and customers, it also results in new challenges. With distribution grid equipment having remote control capabilities and the ability to communicate via a data network, a cyber-attack or other cyber-event can directly result in a grid event, such as an outage or even destruction of equipment. Similarly, two-way communications with customer equipment increases the opportunity for unauthorized access to utility assets. Therefore, in order to have a comprehensive awareness of grid reliability and safety levels, it is now also necessary to consider cybersecurity alongside more traditional concerns, such as the maintenance of physical plant and equipment.

1.2 Utility Systems and Cybersecurity

In the electric utilities context, cybersecurity is usually viewed in relation to two types of assets: information technology (IT) and industrial control systems (ICS).[6] Traditionally, ICS had limited functionality and were isolated from other systems. Due to the requirements of the modern grid, ICS are becoming more sophisticated and integrated with IT systems. The result is a highly complex system architecture consisting of devices, communication networks and software. Cybersecurity must be designed-in these new integrated systems, along with supporting organizational and personnel policies. Notably, while many IT networks operate in a world where interruptions in availability are typical, the ICS network operates at a much higher level of reliability. The merging of these two networks poses even more basic reliability questions as ICS networks become more reliant upon IT networks.

1.3 Cyber-Attacks and Risk

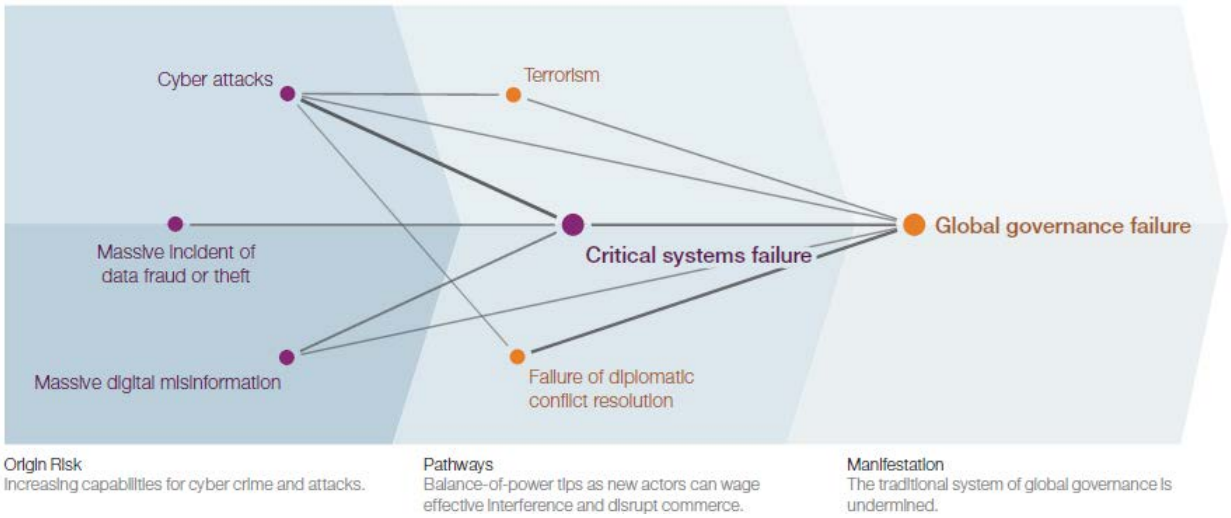
Cyber-attacks on critical energy infrastructure can be used as an unconventional form of modern warfare. Complexity of the systems and the resulting increased opportunity for operator error can result in the same level of damage as intentional attack. Terrorism, disgruntled employees, inadvertent errors, software bugs, Internet pranksters, organized cybercrime entities, or international cyber-warfare have equal potential to compromise or destroy expensive equipment or steal confidential information. These attacks can result in loss of life or life-threatening conditions across wide geographies, the loss of critical infrastructure, and massive property or revenue loss.

Figure 2 illustrates how risks in the cyber-sector are related to larger scale risks of critical systems failure, terrorism and ultimately, global governance failure. Political actors and

[6] An ICS is a system of hardware and software resources that directly manage the behavior of devices in the electrical grid, such as a SCADA system.

others can use these relationships to destabilize systems as new vulnerabilities in critical infrastructure become evident. Both regulators and utilities need to be cognizant of the broad reach of electrical system cyber vulnerabilities and threats, and how the impact of attacks can extend into risks in the broader spheres of political stability and governance. When making risk assessments it is prudent for regulators and utilities to consider these broader implications when determining appropriate allocation of resources.

Figure 2: Relationship of Cyber-Crime to Other Risks[7]



Utilities usually make an assessment of the risk of attacks or failures on the basis of:

a. threats,
b. vulnerabilities,
c. impacts, and
d. frequency or probability of occurrence.

It is useful to understand the distinction between threats and vulnerabilities. A threat is the potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system. Vulnerabilities are specific weaknesses at any link in the chain of security controls or measures that can be exploited by a threat source. An example is the difference between leaving a door to your house unlocked (creating a vulnerability) and the presence of burglars in your area (who pose a threat). Impacts can be both quantitative, such as revenue lost, and qualitative, such as negative press. Finally, the frequency or probability of an attack or failure is an important input for assessing the overall importance of a risk. There are several models that exist for risk quantification, such as Annual Loss Expectancy calculations, that can be used as part of quantitative risk analysis.

[7] Price Waterhouse Coopers, *Op.Cit.*

1.4 Potential Impact of a Cyber-Attack on a Utility System

Without an integrated approach to cybersecurity, attacks or accidental events can cause a cascade of grid reliability events that can amplify the disruption caused by an IT security breach. The following scenario[8] illustrates the potential effect of a cascade of cybersecurity events:

> Insiders mistakenly leave open secure data ports during system maintenance enabling outside access to data on load and generation being provided to the ISO. Outside groups, who are constantly probing the utility, discover the vulnerability and hijack the data communications. This allows them to insert erroneous data, through a "man-in-the-middle" exploit, causing a regional blackout. When the erroneous data is discovered, operators need to base operations on conservative estimates because they can no longer rely on the instrumentation data they receive. This results in expensive dispatch decisions based on these inaccurate estimates. The data hijacking quickly becomes more widespread, further wreaking havoc with generation and transmission operations.
>
> At nearly the same time as the data hijacking, massive denial of service (DOS) attacks flood the email systems of the utilities, causing impairment of communications at all levels within the utility. The clogged email systems further interfere with the utility's ability to respond to operational problems that are due to the hacker exploit.
>
> As utility operations become more chaotic, substations in the region are subjected to cyber-attack, using a previously unknown "back-door" in an ICS operating system, which causes the automated control and monitoring functions to malfunction and damage equipment. This equipment is also required to deal with the operational changes needed because of compromised ISO-level communications. The substation failures are caused by modified system firmware in programmable controllers that have been reprogrammed by hackers. The coordination required to conduct forensics to correct the problem and identify the attackers has been severely impeded due to the disabled email system and compromised networks. Insider attacks on the utilities' internal networks further complicate response.

Not only can vulnerable IT systems result in grid reliability issues, but they can also allow the widespread release of private customer information and usage data. Unauthorized disclosure of customer data can lead to knowledge of customers usage patterns, whether a customer is home or not, or harassment by individuals or other companies. Privacy is a basic customer

[8] Adapted from "Cybersecurity for State Regulators," National Association of Regulatory Utility Commissioners, June 2012.

protection principle; ensuring that private customer usage information is kept secure is a fundamental premise for that principle.

1.5 Examples of Cybersecurity Events in the Energy Industry

1.5.1 Stuxnet

Cybersecurity events in the utility and related industries have already taken place. Stuxnet is a computer worm that was discovered in June 2010. Stuxnet is an example that shows how control systems can be hijacked by a cyber-attack via malware, causing operational disruption and even destruction of equipment, whether or not that system is connected to a network. Stuxnet initially spreads via Microsoft Windows and targets ICS and other equipment, such as SCADA systems. The attacks are manufacturer specific, targeting systems developed by Siemens. Stuxnet gained world-wide attention when it caused significant damage to nuclear centrifuges at a facility in Natanz, Iran. Recently a newer, more complex and sophisticated software worm called Flame has been uncovered. It shares some commonalities in code with Stuxnet and appears to have been created for a similar purpose, but has greater capabilities for compromising systems.

1.5.2 Aurora

The vulnerability of power generation equipment to cyber-attack was demonstrated by the Aurora event, which was staged in March 2007, by United States security officials at the Department of Energy (DOE) Idaho facility. This attack on a vulnerable generator control system caused destruction of the generator and a fire.

1.5.3 Smart Meter Hack

Smart Meters have also been attacked by cyber-criminals. For example, a 2010 report from the Federal Bureau of Investigation (FBI) revealed that Smart Meters in Puerto Rico have been hacked by exploiting a vulnerability in an optical computer access port in the meter used for maintenance. The meter memory could be modified to reduce the electricity use reported by the meter, which enabled electricity theft.

1.5.4 RuggedCom

Another recently reported vulnerability can potentially affect ICS globally. Known by the software manufacturer's name, RuggedCom, this vulnerability provided an easily accessed "back door" into the basic operating system used for device control in numerous systems used in the utility and other critical industries. Although there are no known instances of hackers exploiting this vulnerability, its disclosure forced the company and its customers to scramble to close this critical security gap. California utilities are among the customers affected by this vulnerability.

1.5.5 Shodan

Shodan is an Internet search engine that sought to identify devices that are linked to the Internet. Users of the search engine discovered that many devices were connected to the

Internet unintentionally and usually with minimal security provisions. Notably, users discovered that many ICS devices, such as pump controllers at municipal water plants and utility SCADA networks, were connected to the Internet unbeknownst to the operator. Additionally, many of these devices have little or no security; typically no more than a simple factory-set password that the user usually does not change. The danger exposed by Shodan is that ICS devices, which have relied on security by obscurity, are becoming known and controllable through their interaction with the Internet, even when the user is unaware that the device is connected to the Internet.

1.5.6 San Onofre

On August 16, 2012, The Nuclear Regulatory Commission (NRC) reported that Southern California Edison (SCE) failed to safeguard the sensitive security equipment at San Onofre nuclear plant from hackers and other cybersecurity threats. According to NRC, SCE failed to develop proper procedures for analyzing cyber-threats for electronic devices that use information related to the physical security of the plant's twin reactors. While SCE has since resolved the issue, this incident highlights the potential vulnerability of the electrical power grid.

2 Government's Role in Cybersecurity

The electrical grid is a national security asset and therefore, ensuring cybersecurity of the grid is a significant consideration at all levels of government. As the electric industry undergoes a transformation through grid modernization to a "Smart Grid,"[9] the advanced communication and automation technology necessary will increase its vulnerability to cyber-attacks. As the result, there is an increasing need for government to validate and monitor the security of the communication and computing systems being installed throughout the utility networks.

Cybersecurity of the electric grid falls under the rubric of national security; therefore, all levels of government have been involved in ensuring the security of both IT systems and critical infrastructure. This is appropriate, yet it creates jurisdictional challenges, particularly for the electric industry, since both State and Federal government have regulatory responsibilities in the grid and bulk power system[10].

[9] "Smart Grid" generally refers to a class of technology being installed to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. (from the Smart Grid Information Clearinghouse, http://sgiclearinghouse.org).

[10] *"…all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy."* Phase II draft of Revision of Bulk Electric System definition, NERC Glossary of Terms.

2.1 Cybersecurity Planning

Since security and emergency response are linked, planning and regulatory actions related to cybersecurity have taken place in 1) reducing risk associated with threats and vulnerabilities, and 2) planning for the potential impact of, and recovery from, attacks or accidents. In addition, governments have taken an active role in guaranteeing privacy of personal information.

Security planning efforts generally are oriented toward both anticipating events through risk mitigation, and mitigating the effects of the occurrence of events that threaten public safety, whether they are accidental or intentional. Thus, cybersecurity planning for utilities involves both prevention and reduction in likelihood of damage or destruction of critical systems that impact the safety and reliability of the grid, as well as coordinating with the overall response when these systems are compromised. Another essential element of cybersecurity is protection of sensitive information, including private customer information.

2.2 Legislative Action in Cybersecurity

Legislators are actively involved in creating cybersecurity related laws, both at the Federal and State levels. Until recently, there were two cybersecurity related bills being considered by Congress. The first bill is S. 2105, the "Cybersecurity Act of 2012" (Sen. Lieberman I-CT), which calls on the Department of Homeland Security (DHS), in collaboration with other Federal agencies and grid owners and operators, to asses cybersecurity risks for the country's most critical infrastructure and craft standards for protecting the system. The second bill is S. 3342, the "SECURE IT Act" (Sen. McCain R-AZ), which would, among other things, make it easier for companies to share information about cyber-threats with each other and with the government. Prior to these bills, S. 1342, the "Grid Cyber Security Act" (Sen. Bingaman D-NM) would amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities by, in part, expanding the authority of the Federal Energy Regulatory Commission (FERC). It is now being considered as a potential amendment to S. 2105.

Recent action in Congress stalled these bills and any near term action on cybersecurity legislation at the Federal level. As a result, President Obama has announced that he is considering action in the Executive branch, such as executive orders. A recent news article[11] stated that potential actions that could be taken by the President could accomplish many of the same objectives of the legislation such as:

- Encourage operators of key facilities to adopt voluntary standards
- Direct Homeland Security to coordinate with facility operators on standards adoption

[11] Bloomberg News, August 8, 2012, "Obama Considering Executive Branch Action on Cybersecurity"

- Require cybersecurity focus by existing Federal regulators

At the California State level, in 2002, the legislature passed SB 1386 (Peace) which requires that any company that maintains personal information on a Californian must disclose the details of any unauthorized release of that information. Subsequently, in 2010, the legislature passed SB 1476 (Padilla) which provided rules to protect the privacy and security of customer data generated by advanced meters. The CPUC subsequently issued Decision (D.)11-07-056 on July 28, 2011 which implemented SB 1476.[12] In adopting these rules, CPUC directed the utilities to insure that customer usage data generated by advanced meters is both secure and kept private, and to notify their customers about how customer usage information is used by the utility and with whom a utility may share customer usage information. The rules also provide additional guidance in the event of a privacy or security breach affecting customer usage information.

2.3 Federal Regulatory Bodies and Standards

There are a number of agencies and standards bodies that are working on both cybersecurity of non-industry specific critical systems (both cyber and physical), and cybersecurity specifically related to the power grid. On the Federal level, the DHS has created the Computer Emergency Response Team (US-CERT) which has taken the lead in defining best practices for securing enterprise IT systems as well as control systems (ICS-CERT). The Federal government has also recognized the importance of cybersecurity the electric power industry in particular. The first major step was taken in the Energy Policy Act of 2005, which authorized a self-regulatory "electric reliability organization" that would span North America, with FERC oversight in the United States. The legislation stated that compliance with reliability standards would be mandatory and enforceable. Consequently, NERC became the "electric reliability organization" in the United States.

2.3.1 NERC Critical Infrastructure Protection Overview

Following its establishment as the electric reliability organization, NERC developed CIP standards that require the utilities to put a baseline set of security measures in place intended to protect the bulk power system. Currently, NERC-CIP is the only mandatory requirement that must be met by the electric utilities in the area of cybersecurity related to operations, outside of customer data privacy. NERC-CIP has the following nine sections:

- CIP-001 Sabotage reporting
- CIP-002 Critical Cyber- Asset Identification
- CIP-003 Security Management Controls

[12] Both SB 1476 and D.11-07-056 follow the Fair Information Practice Principles. See "Fair Information Practice Principles," Federal Trade Commission (last updated June 25, 2007) (available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm); "Privacy Policy Guidance Memorandum," Department of Homeland Security (December 29, 2008).

- CIP-004 Personnel and Training
- CIP-005 Electronic Security Perimeter
- CIP-006 Physical Security of Critical Cyber- Assets
- CIP-007 Systems Security and Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Plans for Critical Cyber- Assets.

In essence, these standards require the entities that "materially impact" the reliability of the bulk power system, such as transmission and generation operators, to:

- Report incidents determined to be deliberate attempts at sabotage of bulk power system operations
- Identify critical cyber-assets associated with critical assets of the bulk power system
- Implement a minimum set of cybersecurity policies and controls in the organization of the Responsible Entity
- Deliver required training for personnel that have physical and/or cyber-access to critical cyber-assets
- Define an Electronic Security Perimeter within which assets will have specified protected cyber-access
- Define a Physical Security Perimeter within which assets will have specified protected physical access
- Specifies "methods, processes, and procedures for securing those systems determined to be Critical Cyber- Assets, as well as the other (non-critical) Cyber- Assets within the Electronic Security Perimeter(s)"
- Identify, classify, respond to and report Cyber- Security Incidents related to Critical Cyber- Assets
- Put recovery plan(s) in place for Critical Cyber- Assets. These plans must follow established business continuity and disaster recovery techniques and practices

Non-compliance with any of these requirements can result in a penalty of as much as a million dollars a day. Compliance is enforced through a variety of mechanisms, including self-certification and periodic audits.

2.3.2 Limitations of NERC-CIP

Although NERC-CIP established mandatory requirements, there are vulnerable areas of utility operation that it does not cover. For example, NERC-CIP currently applies only to the bulk power system, which excludes any elements that only serve local load, are part of a local network, or are located on the distribution side of the power grid. This has traditionally been the jurisdictional boundary between State and Federal regulation. However, the operations of the utilities that occur in the distribution grid that involve cyber-assets are

numerous, including the advanced meters, instrumentation data from distribution substations, substation protection relays, and the communication network between utility assets, to name a few. Indeed, in California, the entire sub-transmission network of 100kV and below falls outside of NERC-CIP requirements, as well as approximately over 266,000 miles of conductors, 10,000 distribution circuits and 1000 substations serving nearly 15 million customers[13].

Since NERC does not regulate the distribution system, it does not have the ability to implement cybersecurity requirements in this area. However, this may change. There has been some interest at the Federal level, as well as in the industry, in moving to NERC regulation of cybersecurity in the distribution system. There is also a possibility that the Federal government could preemptively move to regulate in this area if there is no action at the State level.

2.3.3 NRC

After the terrorist attacks of September 11th, 2001, the NRC ordered its nuclear power plant licensees to enhance their overall security. The order included specific requirements for addressing certain cyber security threats and vulnerabilities. Subsequently, NRC issues several other orders and took other important steps in enhancing cybersecurity for nuclear power plants, such as publishing a self-assessment tool for use by nuclear power plants. In March 2009, the NRC issued a new cyber security rule. This new section of the NRC Code of Federal Regulations, "Protection of Digital Computer and Communications Systems and Networks" (10 CFR 73.54), affected existing nuclear power reactor licensees and those corporations applying for new reactor licenses. The new regulation requires licensees to submit a new cyber security plan and an implementation timeline for NRC approval. Most recently, in January 2010, the NRC published a Regulatory Guide that provides comprehensive guidance to licensees and applicants for licenses on an acceptable way to meet the requirements of N10 CFR 73.54. The guidance includes recommended best practices from such organizations as the International Society of Automation, the IEEE, and the National Institute of Standards and Technology (NIST), as well as guidance from the DHS.[14]

2.3.4 NIST and Smart Grid

The Federal government is taking action on developing voluntary, consensus standards as well. The NIST is part of the Department of Commerce and is responsible for defining measurements and standards for the Federal government. As part of the Energy Independence and Security Act of 2007, Congress directed NIST to begin a process to bring together the disparate stakeholders working on Smart Grid to review, develop and reach

[13] Data compiled from IOU corporate reports, California Energy Commission and EIA.
[14] Summary of NRC is adapted from the NRC website https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cybersecurity-bg.html

consensus on standards that apply to the Smart Grid. NIST created the Smart Grid Interoperability Panel (SGIP) to meet those directions. The SGIP is an open, stakeholder-driven process that identifies:

a) existing standards related to Smart Grid,
b) gaps in those standards and needs for standards specific to Smart Grid, and
c) key areas of special review.

One area that was identified for special review was that of cybersecurity and privacy, which resulted in the creation of the NIST Interagency Report (NISTIR) 7628.

2.3.5 NISTIR 7628

The current work being done by NIST in the area of cybersecurity is in the form of recommendations or guidelines. The most prominent example of this type of recommendation is NISTIR 7628, *Guidelines for Smart Grid Cyber Security*. This document identified the need to include cybersecurity in Smart Grid investments as a designed-in feature. Since its publication, NISTIR 7628 has become a useful tool for those working on cybersecurity in the energy sector, noted for its comprehensiveness and utility. In addition, NISTIR 7628 lead to the creation of the Cybersecurity Working Group (CSWG) which is an open forum for Smart Grid stakeholders to review all standards from a cybersecurity perspective. The CSWG suggests modifications to Smart Grid standards to bring them into compliance with NISTIR 7628 guidelines.[15]

2.3.6 DOE Risk Management Process

More recently, the DOE, in conjunction with NERC and NIST, issued a Risk Management Process (RMP) to assist electric utilities in understanding and managing cybersecurity risk in their networks.[16] The RMP is a guideline presenting a risk management model that is tailored for utility operations. The process it describes is based on a three tier structure that addresses risk in the context of:

a. the organization,
b. mission and business processes, and
c. IT and ICS technology.

The RMP recommends that electric utilities use a continuous cycle of framing, assessment, response and monitoring to be able to appropriately manage risk and allocate resources for cybersecurity investment.

---

[15] The CSWG also includes a subgroup focused on privacy and is developing a process to do a privacy review for standards going through the CSWG process.
[16] "Electricity Subsector Cybersecurity: Risk Management Process," Department of Energy (May 2012).

2.3.7 Risk Management Maturity Model

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[17] was developed in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House initiative led by the DOE in partnership with the DHS and in collaboration with representatives of asset owners and operators within the electricity subsector. The initiative used the National Infrastructure Protection Plan framework as a public-private partnership mechanism to support the development of the model. This is a recent development that is intended to allow electric utilities to assess their cybersecurity capabilities and to develop a virtuous cycle of improvement. The model has the following four objectives:

- Strengthen cybersecurity capabilities in the electricity subsector
- Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities
- Enable utilities to prioritize actions and investments to improve cybersecurity.[18]

2.3.8 Other Voluntary Standards

Other standards organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), have weighed in on cybersecurity for electric utilities. IEEE, for example, has published recommendations for electronic and physical security at electric substations.[19] Internationally, the International Electrotechnical Commission (IEC) is also active in standards development for the Smart Grid. For example, the IEC is developing a cybersecurity standard that includes a vendor certification process.[20] In addition, IEC has set up the Smart Grid Strategic Group (SG3), also working with NIST, on developing Smart Grid standards that are normalized internationally. Finally, the International Organization for Standards (ISO) has information security standards (27000-27006) that have come into broader use internationally for securing enterprise data systems.

3 Key Cybersecurity Challenges for State Regulators

Compliance has played a central role in existing government policies on cybersecurity. NERC-CIP, for example, establishes cybersecurity requirements for the bulk power market, and utilities are audited against these requirements. The compliance-based approaches to

[17] "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)," Department of Energy, Version 1.0 (May 31, 2012).
[18] *Id.* at 2.
[19] IEEE Std 1402™-2000 (R2008), IEEE Guide for Electric Power Substation Physical and Electronic Security.
[20] IEC 62443 covers network and system security for industrial-process measurement and control.

cybersecurity, while providing for a baseline amount of security, do not necessarily ensure that utility assets are protected as effectively and completely as is possible at any given time. Recognizing that a 100 percent secure system is not possible, it may in any case be possible to ensure a higher level of security through other approaches.

3.1 Constantly Changing Threats and Vulnerabilities

Given the dynamic nature of cyber-threats and vulnerabilities, it is difficult or impossible to specify a static set of security requirements and controls that will adequately protect all critical infrastructure and related information systems for all time. As technology changes, techniques for ensuring that technology is secure against unauthorized access or abuse will also change. For example, so-called "day 0 exploits"[21] will emerge that use previously unknown or undiscovered vulnerabilities in hardware or software to attack critical infrastructure or information. It is vital that utilities have policies and practices in place that allow them to respond quickly to such threats. Just as importantly, there need to be incentives in place for the technology providers to address security issues and support the utilities as they manage the emerging threats and vulnerabilities. Individual utilities often lack market power to influence the technology providers to resolve specific concerns and this is an area where regulators can play a supportive role for the utilities to help correct the issues.

3.2 Instrument Control and Embedded Systems Challenges

Another emerging issue related to Smart Grid and electric utility cybersecurity is that of securing automated equipment used to control and monitor critical systems. ICS, SCADA and other embedded control systems employ software or firmware that can be compromised. As the control and monitoring of grid-related functions becomes more deeply integrated into utility business practice, it becomes more difficult to separate "information technology" cybersecurity from operational security. Ongoing assessment of the risks associated with automated equipment, particularly as it is installed or upgraded, is an essential part of any cybersecurity plan.

3.3 Greater Organizational Integration

Procedures used by organizations within a utility need to have an integrated security evaluation. For instance, IT networks and computer software may be "patched" or updated only on a regular basis, rather than immediately when problems are discovered in networked ICS equipment. This may lead to a delay in addressing or responding to a vulnerability. Thus, the integration of not only the utility functionality via computer networks, but also the various departmental procedures, in this case IT and operations, inside a utility

[21] Day 0 exploit refers to cyber-attacks that exploit a vulnerability that was unknown to the vendor or developer of the vulnerable system until the time of the attack. Typically this exploit occurs as a result of insider knowledge.

interacting with those networks, will also be needed to facilitate a robust approach to cybersecurity.

3.4 Voluntary versus Mandatory Security Measures

The development of standards for the purpose of securing utility cyber-assets has not been lacking, as discussed earlier. The issue is how best to use the standards and best practices and to monitor their use by the utilities and the vendors. A potential problem may exist in expecting utilities and technology providers to voluntarily comply with standards designed to protect public safety against high impact, low probability events, at significant cost. As James Lewis, director of the Technology and Public Policy Program at Center for Strategic and International Studies (CSIS), points out, "The issue isn't a lack of standards," he says, but rather "It's the lack of a business case for individual companies to spend for public safety. This [AGA-12 case[22]] just confirms it. They know what to do to make things secure and have chosen not to do it for sound business reasons. A voluntary approach doesn't work." This instance demonstrates that a compliance-based approach may be one essential part of ensuring the safety and reliability of the grid. However, a truly comprehensive cybersecurity solution must go farther.

It is important to note that the issue of individual companies having a business case to address cybersecurity applies not only to the utilities, but just as importantly to the vendor companies, or technology providers, that produce the technologies being deployed. The technology companies often cannot make internal business cases to invest in cybersecurity as a part of a product development lifecycle and also cannot change their products fast enough to keep pace with new insights into cybersecurity. Technology companies will generally not enhance or add features to products until there is a compelling market case based on demand across a region and in some cases globally. The resulting problem facing utilities is that they do not necessarily represent a large enough market share to drive vendors to incorporate the utilities' specific cybersecurity needs.

The lack of incentives for technology companies and utilities is an important consideration for all regulators. From this perspective, some compliance-based approach, especially at the Federal level, can be beneficial. However, it is possible for regulators to create compliance regimes that force the utilities and technology companies to allocate resources non-optimally, particularly given the rapidly changing landscape of threats and vulnerabilities. In other words, by requiring technology companies and utilities to comply with a set of requirements, the companies are likely to focus on minimizing the cost of compliance rather than addressing critical vulnerabilities that may involve a higher cost. Therefore, ongoing risk assessment and management practices by the utilities should form a core element of their cybersecurity practices, and regulators should be cognizant of the need for such an approach.

[22] A data communications encryption standard developed for use in critical infrastructure that was dropped by the utilities because of cost.

Regulators must also be able to adapt their assessments of cost-effectiveness to a dynamic assessment of risk. Using risk assessment can greatly enhance the ability of regulators to determine appropriate level of funding for cybersecurity measures, recognizing that a 100 percent secure system cannot be achieved.

3.5 Risk-based Approach to Cybersecurity

Moving to a risk-based approach to cybersecurity allows regulators, and utilities, greater flexibility in determining specific cybersecurity controls or policies. A risk-based approach to cybersecurity allows utilities the ability to focus on areas of their systems that have the greatest impact on the safety and reliability of their systems, and focus funding on appropriate safeguards to mitigate risks to an acceptable level. Allowing the regulated entities to assess risk and allocate resources to security based on risk assessment, if properly structured, can complement a more proscriptive, compliance-based approach.

The challenge for State regulators in relying on risk-based approaches to cybersecurity is becoming comfortable with risk quantification, working with the utility on their risk assessments and methodologies, and understanding that neither a risk-based approach nor a compliance-based approach can reduce cyber-events to zero. Cybersecurity events will occur; including a risk-based approach provides a better means to prevent, and/or respond to a cyber-event. Additionally, State regulators will need a more complete understanding of the costs associated with meeting these cybersecurity challenges in order to determine that spending based on a risk assessment approach is reasonable and effective.

3.6 Including Cybersecurity in Grid Modernization Design Process

With the growth in advanced technologies installed in and impacting the distribution grid, State regulators inevitably will play a greater role in ensuring that the investor-owned utilities have adequate processes for addressing potential cybersecurity impacts and that those technologies contain some level of cybersecurity protections. Retrofitting installed technologies to address cybersecurity is not only less effective, but also a more costly option.

Indeed, including cybersecurity as part of an initial roll-out of technology reduces the need for a utility to retrofit a technology to address cybersecurity after it has been installed, reducing overall costs. Grid modernization and migration to Smart Grid technologies must have cybersecurity designed-in, in order to ensure proper integration and cost/risk minimization. State regulators can play an early role in ensuring that security is an essential element included in planning for Smart Grid deployment. As part of understanding the impact of cybersecurity practices on utility investments in advanced technologies, regulators need to have:

a) an adequate understanding of those practices,
b) the effects of the practices,
c) the associated costs, and

d) in a risk-management program, knowledge of the inputs into the risk assessment methodology.

3.7 The Need for Information Sharing

Effective information sharing on cyber-threats, vulnerabilities and especially cyber-events presents another challenge. In order to learn the effectiveness of strategies to prevent breaches, incidents of failure of security measures must be made broadly available among responsible parties. In addition, detailed information regarding effective measures to prevent attack can boost the security level of the industry generally with the proper forum. State regulators should be involved in information sharing, in order to remain apprised of the current situation, and relevant industry activities. In addition, regulators should have access to all reports of cyber-attack in order to monitor response and recovery.

Notwithstanding the need for information sharing, regulatory involvement may lead to unwanted exposure of sensitive data due to the provisions of the Freedom of Information Act and the California Public Records Act. State regulators and the CPUC will be challenged to create the appropriate forum for information sharing regarding cybersecurity issues, while abiding by the provisions of the public information laws. It may be useful to update existing rules to allow regulators the ability to obtain and maintain the confidentiality of sensitive security information to ensure that such data cannot be released publicly, thereby putting the safety and reliability of the grid into jeopardy.

Additionally, utilities have shown reluctance in sharing with regulators specific documents or reports on cyber-events due to the potential for utility liability should those events result in degradation of service or loss of service entirely. In order to lower the risks and barriers to sharing information with Commissioners and CPUC Staff, safe harbor provisions may be useful to open up lines of communication between utilities and the CPUC. Safe harbor provisions, coupled with new protections around public disclosure of sensitive data, could result in a beneficial exchange of information and a greater openness between utilities and the CPUC.

Finally, the utilities are greatly limited in their ability to share the cybersecurity information that is technology specific. Technology companies are naturally concerned with safeguarding proprietary information and disclosing any potential issues that can give their competitors an edge. As a result, most standard contracts between utilities and technology companies, particularly with early-stage technologies, include non-disclosure agreements that may prevent the utilities from sharing any information regarding cybersecurity vulnerabilities outside of the company, including with other utilities that might also be using the equipment. Not only is this a barrier to the flow of important cybersecurity information, but it also results in increased costs, as each utility has to perform essentially duplicative testing on the same technologies or may suffer loss due to a vulnerability for which there is a solution. Again, individual utilities are constrained in their ability to negotiate these terms, as

their concerns are not necessarily shared by the vendor's general customer base. Overcoming this barrier and allowing the utilities to share information about cybersecurity best practices, events and experiences with other utilities, vendors and other participants would greatly enhance the ability to detect, respond and react to potential cybersecurity threats.

4 Emerging Role of State Regulation in Cybersecurity

As discussed earlier, the Federal government has the only mandatory requirements (NERC-CIP) for cybersecurity that apply to the electric utilities. At present, these requirements only apply to the bulk electric system, which is regulated by the Federal government. NERC-CIP does not apply to the distribution grid. This distinction has traditionally created a jurisdictional "bright line" in regulatory responsibility. Therefore, the State regulators are responsible for filling any cybersecurity regulatory policy vacuum that might exist for the distribution grid, absent action by the Federal government.

4.1 Evolving Role of State Regulators

State regulators have not been traditionally involved in cybersecurity, but this is a trend that has been changing with grid modernization efforts. In 2010, the National Association of Regulatory Utility Commissioners (NARUC) recognized this trend by passing the "Resolution Regarding Cybersecurity" which called for "continued vigilance against all potential sources of cyber-threat to be both prepared to prevent cyber-attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety, and the economy."[23] Key tenets of the resolution encourage Commissioners to:

a. *prioritize the consistent monitoring and evaluating of cybersecurity in collaboration with agencies having expertise in cyber-threat management and mitigation to remain effective in meeting changing cyber-challenges;*

b. *open a dialogue with their regulated utilities to ensure that these organizations are in compliance with standards, and where applicable, ensure that cost-effective protection and preparedness measures are employed to deter, detect, and respond to cyber-attacks, and to mitigate and recover from their effects;*

c. *become and remain knowledgeable about these (cyber-) threats, and ensure that their own staffs have the capability, training, and access to resources to adequately review and understand cybersecurity aspects of filings by their jurisdictional utilities;*

[23] "Resolution Regarding Cybersecurity," National Association of Regulatory Utility Commissioners (adopted February 17, 2010).

d. *revisit their own cybersecurity policies and procedures "to ensure that they are in compliance with applicable standards and best practices."*[24]

In addition, NARUC recently published an extensive cybersecurity guideline for State regulators which calls for proactive action on behalf of State regulators, including:

- Create cybersecurity expertise within their own organizations
- Ask the right questions of utilities
- Assess their own cybersecurity and information protection capabilities
- Engage with other efforts: led by the private sector, State agencies or federal officials and engaging with processes that link these sectors.[25]

4.2 Example of State Regulatory Action: California

The CPUC has been proactive in cybersecurity policy in several areas. First, the CPUC has actively participated in the development of the Urgent Action Cyber Security Standard 1200 (UA 1200) that was adopted in 2003 as a temporary standard prior to the development of the NERC-CIP standards. Subsequently, the CPUC continued its involvement in the development of current NERC-CIP standards though filing comments and voting. The CPUC staff continues to be involved in the development of a many standards pertaining to reliability and security in general.

In another notable step, in July 2011 the CPUC issued D.11-07-056 which provided a number of privacy protections for customer usage data generated by advanced meters. With data generated by advanced meters, third parties may seek to obtain customer usage and offer customers, with their consent, additional services beyond utility offerings. States have a clear interest and authority in overseeing that customer usage information collected by advanced meters is being used in a manner that protects customers' privacy. These rules govern the use of customer usage data by the utility and third parties under contract with the utility. The CPUC was the first State commission in the United States to issue rules specifically on data generated by Smart Meters. Subsequently, the Colorado Public Utility Commission and the Public Utility Commission of Texas have also finalized rules on customer privacy. Several other States currently have open proceedings investigating issues related to privacy, including Michigan, Ohio, and Vermont.

Additionally, the CPUC has taken initial steps in ensuring that cybersecurity is addressed in grid modernization efforts. Senate Bill (SB) 17[26] required the CPUC to work with stakeholders to determine requirements for utility Smart Grid deployment plans. The

[24] *Id.*
[25] "Cybersecurity for State Regulators," National Association of Regulatory Utility Commissioners, June 2012.
[26] SB 17 (Padilla), Chapter 327, Statutes of 2009.

deployment plan requirements included cybersecurity and cybersecurity strategy. The deployment plan decision states:

> *Although the issues of grid security and cyber security could be addressed as part of the strategic planning section, this decision requires that deployment plans include a separate section on the topic of security. The section on security will require the utility to discuss the security needed to ensure the operation of the grid and the security needed to prevent unauthorized access to consumer data.*[27]

As required by SB17, the utilities filed their Smart Grid deployment plans in June 2011 and are currently pending before the CPUC. These plans contain the required sections on cybersecurity and privacy.

4.3 Example of State Regulatory Action: Michigan

In December 2011, the State of Michigan released "The Smart Grid Collaborative Report to the Michigan Public Service Commission (MPSC)." The Collaborative was created by order of the MPSC in April 2007.[28] The purpose of the Collaborative was "…to review national Smart Grid infrastructure development, determine cost-effectiveness and practicality and establish evaluation criteria and standards, thus triggering pilot programs or broader deployment in Michigan. The Collaborative was instructed to focus on making the grid flexible and efficient, enabling distributed technologies, and preserving reliability."[29]

The Report is a high-level strategy document containing recommendations to guide the planning for Smart Grid deployment. The Report recommends that utilities be required to use NISTIR 7628 for implementation of cybersecurity in their Smart Grid deployment. However, at this time, MPSC has given no regulatory direction on specific cybersecurity requirements.

4.4 Example of State Regulatory Action: Pennsylvania

The Pennsylvania Public Utility Commission (PA PUC) has issued orders and regulations regarding cybersecurity of their electric utility. Under Pennsylvania Utility Code 52 Chapter 101[30], jurisdictional utilities are required to maintain Physical Security, Cybersecurity, Emergency Response and Business Continuity Plans, and to self-certify that they have complied with the regulations. Utilities do not submit the plans to the PA PUC, but PA PUC staff may review any or all parts of the plans at any time. According to PA PUC Staff,

---

[27] D.10-06-047 at 29.
[28] Docket No. U-15278, Order Commencing Proceeding, April 24, 2007, http://efile.mpsc.State.mi.us/efile/docs/15278/0001.pdf.
[29] *Ibid.* at 2.
[30] PA PUC 52 §101 Public Utility Preparedness through Self-Certification

"The Code is not particularly lengthy or proscriptive; rather we established minimum plan requirements and required the utilities to develop the plans." [31]

In 2009, the PA PUC issued an Order that "reminded our utilities that our regulations require cybersecurity down to the meter, which is beyond what the NERC CIPs cover."[32] There have also been recent regulation changes[33] which now require reporting of cyber and/or physical attacks that cause over $50,000 in damage and/or any customer service interruptions. Before this change, utilities were not required to report cyber or physical attacks. This applies to electric, gas and water/wastewater utilities.

PA PUC Staff stated, "In terms of review, for the larger utilities (any electric, gas, or water utilities over $10 million in yearly revenue), a review of the four plans for sufficiency is included in our management audit process. Management audits are required to be completed at least once every five years, but there are also management efficiency investigations and other interim audit procedures that look at the four plans. Any findings on the plans are made known to the PA PUC and utilities must address those findings."[34]

4.5 Example of State Regulatory Action: Texas

The Public Utilities Commission of Texas (PUCT) Substantive Rule 25.130, "Advanced Metering," requires advanced meter data to be "consistent with data availability, transfer and security standards adopted by the independent organization or regional transmission organization."[35] The rule provides that if no such standard has been adopted, then the PUCT may specify the standard. The rule further states, "An electric utility shall use industry standards and methods for providing secure customer and [Retail Electric Provider (REP)] access to the meter data. The electric utility shall have an independent security audit of the mechanism for customer and REP access to meter data conducted within one year of initiating such access and promptly report the results to the commission."[36] Although the rule requires an initial security audit, there is no provision for ongoing audits or reporting of security testing.

---

[31] From email communication with Daniel Searfoorce, Emergency Preparedness Coordinator, Pennsylvania Public Utility Commission, Bureau of Technical Utility Services.

[32] Docket No. M-2009-2104273

[33] PA PUC §57.11(b)(4) defines as a *reportable accident* the following," An occurrence of an unusual nature that is a physical or cyber attack, including attempts against cyber security measures as defined in Chapter 101 (relating to public utility preparedness through self certification) that causes an interruption of service or over $50,000 in damages, or both."

[34] *Ibid.* Daniel Searfoorce email

[35] PUCT Electric Substantive Rule §25.130(g)(1)(G)

[36] PUCT Electric Substantive Rule §25.130(j)(3)

The PUCT also established Project #37944, Project to Investigate Cyber Security of the Electrical Utility Industry.[37] This is an American Recovery and Reinvestment Act of 2009 (ARRA) funded research project that was established to investigate basic issues in smart grid cybersecurity, applicable standards and metrics, best practices, and possible approaches for regulators.

5 Proposed Next Steps for the CPUC

As the utilities modernize the grid and their operations, cybersecurity becomes an increasingly important issue. There are clear gaps in current regulatory policy which potentially expose California residents to cybersecurity risks. As a leader in energy policy and grid modernization, the CPUC is in a perfect position to create first-of-its-kind cybersecurity State regulatory policy. If the CPUC takes action, it can not only potentially protect Californians from safety and reliability threats, but also provide an example for other State regulatory agencies.

5.1 Key Cybersecurity Questions for the CPUC

Key questions that should be addressed by the CPUC include:

- Is cybersecurity being adequately addressed to ensure safety of California residents and reliability of electric service?
- How should the CPUC evaluate utility investments in cybersecurity, especially when investments in almost all assets now have a cybersecurity component?
- How should utility cybersecurity performance be monitored by the CPUC?
- How should the CPUC facilitate information-sharing with utilities regarding cybersecurity, in particular, incident and response reporting?
- How can the CPUC ensure that the statewide integrity of grid cybersecurity is uniform, across the California utilities, with no weak links that could potentially jeopardize the entire system?
- How can CPUC better coordinate with California Independent System Operator (CAISO) on cybersecurity issues to ensure end-to-end safety of the system?

5.2 Consideration of Cybersecurity as an Aspect of Grid Safety and Reliability

The CPUC should take steps to oversee that security is being addressed up-front by the utilities, and is being maintained, consistent with existing standards, industry best practices, and CPUC requirements. In related matters, the CPUC is making a concerted effort to place safety as a core mission of its own and the utility business, and will be taking a greater role in overseeing utilities' efforts to ensure that infrastructure is installed and operated in a safe manner. The CPUC should view cybersecurity as another feature of the safe and reliable

[37] http://www.puc.state.tx.us/industry/projects/electric/37944/37944.aspx

modernized grid. The CPUC can ensure that cybersecurity considerations are applied to both new and existing infrastructure such that safety and reliability are continuously improved; indeed, without security, there can be no assurance that any technology is safe or reliable.

Recently, the CPUC announced that as part of PG&E's upcoming General Rate Case (GRC), the Consumer Protection and Safety Division (CPSD) would investigate PG&E's safety and cybersecurity policies and practices. Included in this investigation, PG&E, as part of their GRC, is to file a safety and cybersecurity risk assessment to support their funding requests. CPSD would investigate whether the funding requests were adequate, supported regulatory mandates and guidelines, and maintained a safe and reliable grid at a reasonable cost. PG&E is scheduled to file their GRC by the end of 2012.[38]

5.3 Options for CPUC Action

Based on the above discussion, there are a number of options for potential CPUC action:

- Require NERC-CIP compliance for the distribution system;
- Adopt or develop another form of compliance-based standard, *e.g.*, based on NISTIR 7628 recommendations;
- Develop its own set of rules, policies or requirements for cybersecurity compliance;
- Adopt a risk management-based approach that is integrated with the approach to reliability and safety;
- Adopt a set of requirements that would ensure that the electric system is designed to be resilient to cyber-events;
- Create a hybrid approach that combines a compliance-based floor with dynamic risk assessment and management; and/or,
- Develop or adopt a set of metrics and require utilities to report testing results, as well as cybersecurity incidents.

There are other options available to the CPUC regarding cybersecurity policy. To develop a record based on input from utilities, technology companies and other stakeholders, CPUC Staff proposes that it would be prudent to open an Order Instituting Rulemaking (OIR) to investigate these options.

As part of any cybersecurity OIR, the CPUC should address concerns around the ability to protect sensitive documents potentially subject to Public Records Act issue. Confidentiality of documents related to security measures taken by individual IOUs must be maintained.

[38] As evidenced by their recently filed "Notice of Intent to File General Rate Case Application," PG&E expects to include several chapters devoted to safety and risk assessment and planning.

A cybersecurity OIR should be conducted in conjunction with other efforts related to Smart Grid. A good example is the recent creation of a CPUC Staff-led Cybersecurity Technical Working Group to develop metrics, as well as the results from the safety investigation as part of PG&E's GRC. This OIR can then develop generic requirements or policies for utility cybersecurity practices, if necessary.

The CPUC could require that utilities make use of a risk management approach to cybersecurity, and that CPUC Staff work with utilities, and other interested parties, to develop a framework for that approach which would allow the utilities to implement the framework as it applies to them. It is not expected that specific controls be required, as regulations and strict requirements may not allow the utilities the flexibility to respond to events in a timely manner. Rather, the CPUC may require the development of policies or guidelines that can then drive utility cybersecurity practices.

As part of its review of cybersecurity policy, the CPUC should also evaluate the skill-sets and resources needed for CPUC Staff to adequately address cybersecurity.

6 Conclusion

The need for aggressive and effective cyber-physical security throughout the electrical system is clear due to increased "digitization" of the system as well as evolving threats and vulnerabilities. As investments and technologies in grid modernization are made to create a "Smart Grid," increased automation and complexity require that security measures must be designed-in to be as cost-effective as possible. The safety and reliability of the grid to the meter and beyond increasingly depend on cyber-physical security of critical assets as well as the networked automated equipment throughout the system.

The CPUC has a responsibility to ensure the safety and reliability of the grid down to the meter, and to ensure that utilities are prepared for the challenges of grid modernization as it occurs beyond their control. The CPUC also has a responsibility to ensure that ratepayer dollars are being invested effectively in cybersecurity. Both of these responsibilities require an understanding of the risk assessments conducted by the utilities and knowledge of the results. The CPUC has made a good start in requiring the utilities to include a section on cybersecurity in their Smart Grid Deployment Plans.

However, there is precedent and opportunity for the CPUC to do more to fill-in the regulatory gap that exists between compliance-based standards for the bulk electric system, distribution, and the emerging capabilities on the customer side of the meter.

A cybersecurity OIR for the electric grid would enable the CPUC to establish:

- A framework for evaluating the quality of the Smart Grid cybersecurity plans submitted by the utilities and the annual reports moving forward
- Methods for developing a baseline and auditing the effectiveness of both the initial and ongoing investments in cybersecurity
- A protocol for reporting cybersecurity incidents and information sharing regarding breaches and security failures that solves liability concerns[39]
- The ability to perform root cause analysis of security system failures such that both the government and the utility can respond effectively
- A system of security testing or periodic reporting of results of security testing

Cybersecurity is a cornerstone to the utilities providing safe and reliable service to the customers and the CPUC should continue its proactive approach, as it has done through developing privacy rules and other activities.

[39] There is an existing requirement (General Order 166 and 167) for utilities to report incidents causing damage or are the subject of significant public attention.