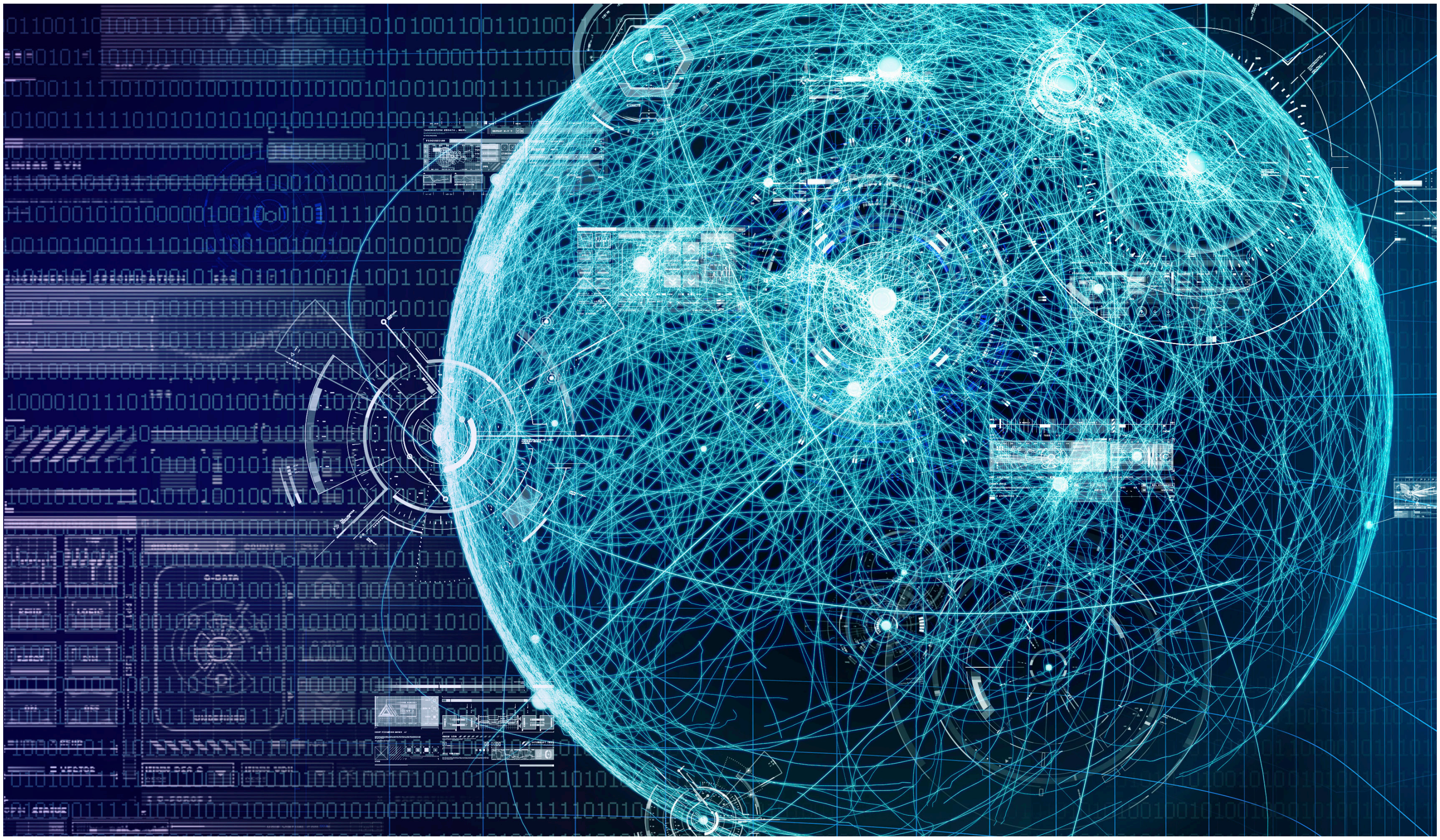
The Heritage Foundation



Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity

Andy Bochman and Steven P. Bucci, PhD

SPECIAL REPORT
from THE DOUGLAS AND SARAH ALLISON
CENTER FOR FOREIGN AND NATIONAL SECURITY POLICY

No. 150 | JANUARY 29, 2014

The Heritage Foundation

Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity

Andy Bochman and Steven P. Bucci, PhD

SR-150

About the Authors

***Andy Bochman** is founder of SmartGridSecurityBlog, The DOD Energy Blog, and Bochman Advisors, LLC, which coaches energy companies, and federal and state agencies that regulate energy companies, on matters of security preparedness, governance, and awareness.*

***Steven P. Bucci, PhD,** is Director of the Douglas and Sarah Allison Center for Foreign and National Security Policy, a department of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

The authors would like to thank Allison Center Research Assistant David Inserra for his help preparing this paper.

Photo on the Cover—
© thinkstockphotos.com

This paper, in its entirety, can be found at:
http://report.heritage.org/sr150

Produced by the Douglas and Sarah Allison
Center for Foreign and National Security Policy

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Table of Contents

SPECIAL REPORT | NO. 150
JANUARY 29, 2014

Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity

Andy Bochman and Steven P. Bucci, PhD

Executive Summary

Over the past decade, the U.S. has witnessed unprecedented transformation of the systems that the electric sector uses to make, manage, and move power. Over the same period, legislators and regulators have become increasingly concerned that utility executives are not doing enough to improve defenses against increasingly numerous and capable cyber adversaries.

Those concerns have manifested themselves in multiple attempts to pass legislation that would mandate new cybersecurity requirements beyond the North American Electric Reliability Corporation's (NERC's) critical infrastructure protection (CIP). In early 2013, the White House issued an executive order that directed the National Institute of Standards and Technology (NIST) to work with industry to create a new cybersecurity framework for critical infrastructure, including the electric sector. While this framework is to be composed of voluntary standards, many are concerned that these standards will eventually be mandatory.

Instead of starting with onerous government regulations, policymakers should start by seeking a better understanding of the current cybersecurity status of the U.S. power grid. This includes:

- An orientation to the grid, including components, technology trends, and key players;
- A review of recent cyber breaches, grid vulnerabilities, and threat actors; and
- An overview of the governance and economics of electric-sector cybersecurity.

Based on these facts, there are practical steps that Congress can take to support and incentivize utility companies as they continue to improve their cyber defenses:

- Encourage utilities to seek better understanding of their current posture and desired future states of preparedness, with an emphasis on executive awareness, measurement, and centralization of control;
- Foster an improved environment for truly collaborative cybersecurity policies, such as information sharing, and use a variety of other tools to facilitate improved government–industry communications; and
- Help the states and their public utility commissions to prepare themselves for fuller execution of their oversight role regarding the cybersecurity readiness of the utilities and grid elements within their borders.

Ultimately, in this domain the utilities control their fate more than they may know. If they can demonstrate that they are becoming more proactive on cybersecurity over time, that positive shift in perception will give Congress and other oversight agencies the assurance they need to let the utilities increasingly determine their own best approaches to cyber-risk management.

SPECIAL REPORT | NO. 150
JANUARY 29, 2014

Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity

Andy Bochman and Steven P. Bucci, PhD

Around the world, and in the U.S. in particular, as people have come to enjoy the many benefits and conveniences of computers, intelligent systems, sensors, smartphones, and modern communications networks, they have also unwittingly created a problem for themselves. The U.S. dependence on these systems puts important elements of critical infrastructure potentially within reach of adversaries, criminals, and nation-state competitors.

To date, the overwhelming majority of reports, articles, and statements by senior government officials have made dire predictions of the catastrophes that will soon befall the economy and country if Americans do not make massive, immediate, and expensive additions to the country's current cybersecurity defenses. Yet, there is little agreement on what types of new protections need to be fielded or how to prioritize spending based on risk and the potential impacts of successful attacks on critical infrastructure sectors.

There are a few other problems with the catastrophic predictions:

- They are based more on speculation than on observation;
- The business case for fear mongering on the part of the cybersecurity–industrial complex tends to skew commentary greatly toward the negative;
- Because few utilities or regulators have found practical methods for understanding the amount of risk in their current cybersecurity postures, senior management and decision makers, while increasingly concerned with this issue, have little insight into the best starting points for improvement; and
- While risk can never fully be managed away, and because there are few tools for measuring the current state of risk or the adequacy of defenses, it is almost impossible to describe a desired future state where risk has been reduced to a level that is aligned with the risk tolerance of business and government.

It seems clear to many that the status quo approach of utilities to securing themselves against cyber threats is no longer adequate. Yet there is, to date, broad disagreement on the actions that should be taken by government and industry to drive demonstrable improvement, including, remarkably, how to recognize improvement if and when it occurs. Many of these challenges and obstacles, however, can and must be overcome.

The Time Is Right for Good Reforms

In the U.S., policymakers have shown a growing interest in increasing government oversight of the cyber components of the electric grid since the great

Northeast blackout of 2003. As a result of the blackout, there were public discussions about the inadequacy of the current grid and how to promote behavior among utility companies that could improve the reliability of the country's electric grid. The massive 2003 incident, while not a result of a cyber attack, nevertheless reminded the country of the fundamental importance of the electric grid, and the risk of cascading failures of massively interconnected systems. As a result, American utilities today are governed by rules from the Federal Energy Regulatory Commission (FERC), interpreted and implemented by the North American Electric Reliability Corporation (NERC) through its critical infrastructure protection (CIP) standards. The rules and regulations are intended to encourage utilities to protect certain parts of the grid in specified ways. Most experts, however, agree that this regulatory approach is not producing the necessary levels of protection.

Because events related to cybersecurity are occurring so rapidly, the following list will likely be out of date by the time of publication. In the past eighteen months alone, the country has witnessed:

- August 2012: *The Economist* featured an exposé of the Chinese telecommunications firm Huawei, describing Western concerns that the presence of the company's control-system products in U.S. telecommunications and energy infrastructure could allow China to disrupt operations in those sectors;[1]
- September 2012: the failure of the Cybersecurity Act of 2012;[2]
- February 2013: the release of Presidential Policy Directive 21 (PPD-21), an executive order on critical infrastructure cybersecurity;[3]
- February 2013: the release of a credible report by security firm Mandiant that connects a China-based military unit to sustained, targeted cyber attacks (many of which were successful in stealing sensitive data) on hundreds of U.S. companies;[4]
- March 2013: cyber attacks of unknown origin that shut down customer transactions at South Korean banks and undermined the operations of a number of South Korean media firms;[5]
- May 2013: revelation of long-running exfiltration by China of classified data from British aerospace defense firm QinetiQ;[6]
- June–August 2013: the Edward Snowden story hits the press, and soon after massive press coverage on the National Security Administration's PRISM surveillance program begins and continues through the summer;[7]
- August 2013: release of the National Institute of Standards and Technology's (NIST's) draft Critical Infrastructure Security Framework (CSF), ahead of a final workshop and issuance of a more formal draft release in October;[8] and
- August 2013: the Syrian Electronic Army hacks *The New York Times,* Twitter, and U.S. Marine Corps websites.[9]

These incidents are sending the cumulative message to the mainstream public, as well as to senior leadership at utilities, federal and state regulators, and other critical infrastructure providers, that the world is full of cyber threats, some of them from very capable sources, and that the federal government is trying to figure out how to help defend the American public (not to mention itself) but so far has not found the right approach.

Nevertheless, for utilities to focus attention and defensive efforts exclusively on one nation-state, one supplier, or on particular adversarial organizations is a mistake. Furthermore, government has a potentially helpful, albeit limited, role to play in this undertaking. So before the nation gets much further down the government-directed path projected by the recent Cybersecurity Executive Order or any of a number of additional pieces of cybersecurity legislation now circulating Capitol Hill, it is important to take a fresh look at the origin of the problems and examine some effective solution candidates.

Orientation: Electricity Grid 101

A rudimentary overview of the electric grid's vast system of systems, as well as some of the many organizations that oversee and operate it, is a must for understanding the cybersecurity challenges facing the nation, and putting them in their proper context.

The U.S. Grid. The U.S. grid has been called the largest machine ever built, as well as the greatest engineering achievement of the 20th century.[10] It is composed of many thousands of generators (powered by coal and natural gas, as well as by nuclear, hydroelectric, wind, and solar power), hundreds of thousands of miles of high-voltage transmission lines and lower-voltage distribution lines, tens of thousands of substations and transformers that regulate and modify voltage, and regional control centers that monitor the quality of electricity as well as fluctuations in the demand that could cause disruptive imbalances and possible outages.

All of this equipment is owned and operated by approximately 3,500 electric utility companies, with regional operational oversight provided by organizations called Independent Systems Operators (ISOs) and Regional Transmission Operators (RTOs). Ten of these regional entities provide coverage for the entire continental U.S., and their most important functions are related to ensuring regional reliability and setting market prices for electricity.

Most utilities' revenue stems from the bills they present to their customers. However, in regulated states, the rates they charge are determined by the state's public utility commission (PUC). A utility can argue for increasing prices by making a rate case—essentially a business justification that explains why it needs additional funding. Often following some negotiation and once approved by the PUC, the new rate is fixed until the next time a rate case is made by a utility.[11]

Deregulated states have created competition so that utilities can adjust the prices they charge customers (who can include other utilities) according to market forces. In Texas, for example, multiple electricity retailers purchase power from non-deregulated companies that provide generation, transmission, and distribution. This means that most power consumers are free to find the best deal and choose their electricity service from a variety of "retail electric providers" (REPs).

Whether regulated or not, however, and allowing a few exceptions, all of the entities that play a role in making, moving, and delivering electricity to customers are interconnected on electricity networks, and increasingly, on data and communications networks used to manage the grid. This means that they share a common responsibility to be cyber-secure, as a successful attack on one could lead to a cascading failure in the electrical grid, or provide adversaries with unauthorized access to the networks and systems of others.

At the national level, cybersecurity oversight is divided between FERC, under the jurisdiction of the U.S. Department of Energy, and the state PUCs. By law, FERC must ensure that adequate cybersecurity defenses are in place in the bulk electric system (BES), essentially the larger generation and transmission assets.[12] This means that the state utility commissions have cybersecurity responsibility for most of the smaller generation and transmission elements, as well as the entirety of the distribution system, which includes the power lines and substations that deliver electricity to rural America and to the largest cities. The amount of cybersecurity expertise in these commissions ranges widely, but it is safe to say that most of them have no staff with any significant cybersecurity training or knowledge.

Utilities share a common responsibility for cybersecurity, as a successful attack on one could lead to a cascading failure in the electrical grid, or give adversaries unauthorized access to the networks and systems of others.

The Smart Grid. Dating back to at least 2005, the term "Smart Grid"[13] is shorthand for a number of technologies that, with the support of the U.S. government, are bringing new capabilities, efficiencies, resilience, and in some cases, new business models, to an industry that has been relatively static for many decades.

In order to gain better insight and control over operations, and achieve higher levels of efficiency and flexibility, systems that used to be isolated from a network point of view are becoming increasingly interconnected. Those that were connected before, such as transmission and distribution substations and the networks that link them to control centers, are trading slower one-way serial connections for high-speed, Internet-based communications. This allows improved two-way communications, and the increased bandwidth gives operators access to much more information about the way their systems are functioning, allowing higher efficiencies and improved responsiveness in the event of trouble.

Another relatively new technology category includes synchrophasors—synchronized phasor measurements that assess power quality many times per second—which are being installed on transmission lines. Providing “wide area situational awareness,” synchrophasors serve as early warning systems for regional grid managers, helping to form a smarter transmission grid.[14]

Of course, to the average person, the most visible indication that something is changing in his relationship to the power company is the new meter on the side of his home or office building. Originally, meters were purely mechanical, and, in order to determine the electricity consumption at a given business or household, a utility employee needed to visit the premises and read the meter. In the 1980s, many utility companies began deploying advanced meters, with automated meter reading (AMR) capabilities which could broadcast their usage, typically using dedicated radio frequencies. These were installed to save utilities the expense of visiting each individual residence. Now they could simply drive down a street and collect all the meter data for a neighborhood without leaving the truck.

More recently, advanced metering infrastructure (AMI), which includes the networks and applications that support smart meters, has become prevalent in many states. AMI networks and smart meters are not only capable of communicating usage information directly back to the utility on a 15-minute or hourly basis, but can also respond to control signals to perform a variety of functions. Benefits for utilities include demand management (the ability to constrain the amount of electricity used by customers during peak demand periods), more accurate meter readings, and the ability to better detect tampering. Consumers benefit from more accurate billing and a better understanding of their electricity consumption patterns, allowing them to save money by shifting their use of large appliances, when possible, to a time when the price of electricity is lower.

While there is a significant amount of heterogeneity in Smart Grid modernization projects across the country, some cybersecurity-relevant characteristics are common throughout:

- The increasing interconnection of formerly independent systems;

- Where connectivity previously existed, substantial increases in throughput are the norm;

- Formerly obscure system-specific communications protocols, that is, a systems of rules for message exchange within or between computers, are being replaced with more standardized ones, particularly Internet protocol (IP); and

- A blending of the concepts, and increasingly, a convergence of the networks and systems, of information technology (IT) and operational technology (OT), the latter composed of the systems that directly support, monitor, and enable control of generators, transformers, and other substation components.

OT used to be an island unto itself requiring only physical security-access-control protections. Now it is becoming increasingly common to find OT systems connected to IT networks, and, even more problematic, directly to the Internet. Worse, individuals are able to search for these Internet-connected systems through a publicly available search engine, known as Shodan (Sentient Hyper-Optimized Data Access Network), making it easy for bad actors to identify potential targets.[15] Overall, greater interconnectivity and the use of more standardized protocols mean that it is easier for hackers to figure out how to infiltrate a system.

Cybersecurity Lessons from Other Sectors

One key aid in the effort to substantially modernize grid infrastructure is that a number of other critical infrastructure industries have already previously undergone similar transformations predicated on new ways of doing business, leveraging computers, and advanced communications technologies. These industries can provide examples for how to secure the electric grid. While there are several aspects that make the electric-power sector unique, there are also many ways in which it can leverage the best practices of, and lessons learned by, these industries, and effect this transformation. As such, key lessons can be learned from the following three sectors:

Financial. Long before the first Web browser was produced, banks were using Information Technology (IT) and Internet-based communication networks to transfer vast sums of money in a business-to-business e-commerce process called electronic data interchange (EDI). As soon as their customers were able to reach the Internet in the mid and late 1990s, pioneering banks and brokerages also began offering their services online. Around the same time, related technologies were used to support the mass deployment of automated teller machines (ATMs). Hand in hand with these new tools came attackers who figured out how to exploit inadequate cybersecurity defenses.

To meet the challenges posed by the many financially motivated attackers, ranging from individuals to organized crime syndicates, the financial services industry responded in a number of ways, including the formation of a collaborative cyber defense group called the Financial Services Information Sharing and Analysis Center (FS-ISAC) and a voluntary set of cybersecurity standards and processes called the Payment Card Industry Data Security Standard (PCI-DSS). Perhaps because its operational business can be considered a massive IT operation, and even though it does suffer breaches and losses on a regular basis, this industry is often viewed as the best at protecting itself from cyber threats. Clearly it has mechanisms in place to learn from new attacks and effectively promulgate information on cybersecurity threats and vulnerabilities throughout the industry.

Telecommunications. There have been three main phases in the evolution of the modern telecommunications system as it exists today. The first was fully mechanical and analog. The second was electronic and digital and used industry-specific or organization-specific rules, known as proprietary protocols. Finally, the one being built and used today increasingly uses more standardized, or standards-based, IT equipment and IP networking. One example is voice-over IP (VOIP). This refers to the standards-based approach for converting analog signals, such as the voice on one end of a phone call, to data packets that are then transmitted across computer networks and reassembled to form the audio heard by the listener on the other end.

Telecommunications companies, also called Internet services providers (ISPs) or communications services providers (CSPs), have been the target of cyber attackers since the minute their systems went digital. The situation is particularly precarious since their infrastructure and services products, data and voice, ride the same electronic pathways that attackers use to reach their targets.

As a result, like the financial services industry, ISPs and CSPs formed their own cyber defense community, the Telecommunications Information Sharing and Analysis Center (ISAC), and the telecommunications sector is now considered to be among the most mature sectors in terms of understanding, and proficiency in, cybersecurity processes and secure control technologies.

Military. The U.S. Department of Defense rounds out the list of the high-functioning cybersecurity sectors. The Defense Department takes credit for the development of game-changing new technologies, and often it deserves it. This is definitely the case for both the development of supercomputers (used to model, among other things, nuclear reactions) and the Internet itself, initially a Defense Advanced Research Projects Agency (DARPA) project.

As the protector of the United States and its interests worldwide, the Defense Department endures a high level of continuous cyber attack, and since there is no other agency it can rely on for help, it must be able to fully defend itself. To this end it maintains a uniform minimum level of cybersecurity preparedness by ensuring adherence to standards established by the NIST federal laboratory. Of NIST's standards, two that form the basis for much of the military's primary cybersecurity guidance document, the Defense Department's Information Assurance Certification and Accreditation Process (DIACAP), also inform the electric-sector standards.[16]

While the Defense Department has a markedly different mission than do financial services and telecommunications companies, most of its computer, networking, and communications gear is built by the same providers; it is therefore not surprising that many of the cyber best practices from any one of these sectors are applicable, and are leveraged, in the others.

Vulnerabilities in the U.S. Grid and Grid Systems

One does not need a security clearance to discover some of the most readily exploited vulnerabilities in the cyber systems that support America's power grid. As it comes increasingly to embrace and leverage Internet technologies, the electric sector cannot but help inherit the problems that come with them. Here is a quick overview of some of the most significant areas of concern.

Grid Security and the Defense Department

The U.S. Department of Defense is charged with protecting the entire country, including U.S. assets and allies around the world—its electricity needs are great. Yet, its grid-related responsibilities are minimal. Illustrating this fact, in 2001 and again in 2008 the Defense Department's Defense Science Board published comprehensive reports on the department's energy challenges and what might be done to meet them.[17]

The top two concerns were dependence on oil, for fueling operational Air Force, Army, Marine, and Navy missions; and the complete reliance of fixed installations with increased critical load demands on a grid with questionable resilience. Spurred by these observations and other lessons drawn from U.S. experiences in Iraq and Afghanistan, the military embarked on multiple energy-efficiency initiatives to reduce fuel demand, and initiated the Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) microgrid program.[18] The core concept under development in the program is a system that can isolate itself when the local grid goes down, and run the base using its own power sources, be they diesel generators, solar panels, wind turbines, or another power source. SPIDERS is currently in pilot trials in Hawaii and Colorado.

Another Smart Grid, microgrid, and energy-efficiency project of note is being conducted at Naval District Washington (NDW), a regional designation that includes Maryland, Virginia, and the District of Columbia. As is the case for SPIDERS, the security architecture is built in by design. The NDW Smart Grid installation energy initiative is based on open standards and is the first region to attain full Fleet Cyber Command accreditation for cybersecurity. This potentially paves the way for other Naval regions to adopt the systems pioneered in the NDW pilots, and it might even be possible to see these capabilities embraced by the other services.[19]

Software. The Smart Grid is being constructed from billions of lines of software code, most of it by developers who have had little or no training in how to write secure applications. Before going into production, their work is tested by quality-assurance personnel who check for functional bugs and performance issues, but—notably—often not security. This means that in many, if not most, applications one can expect to find a variety of vulnerabilities that attackers can use to gain unauthorized access or elevated user privileges. While this condition is certainly true for web applications, more recent attention has turned to vulnerabilities in the software that runs control systems.

Depending on their size, utilities rely on applications from a variety of sources, including:

- Those they build themselves using their internal software development team;
- Applications built for them by third-party development companies;
- Packaged applications installed on the utility's own hardware; and
- Software developed as a service, managed and maintained by a third party.

Furthermore, many utilities have not performed a recent application inventory, and until they do, they will have a great deal of trouble prioritizing and protecting effectively.

There are, however, positive examples of utilities rectifying this situation by conducting security scans across their entire application portfolio. Another encouraging trend can be seen with Smart Meter vendors, most, or all, of whom now regularly assess and improve the security characteristics of their meter software before offering it to utility customers.

Data. One of the by-products of the explosion of smart devices and connectivity is the production of huge amounts of data. Whether customer reactions to time-of-day pricing, impacts of weather on renewable generation and power quality, or dozens of other factors, utilities are being deluged with more and more types of data than they have ever had to deal with before. Additional complexity arises because some of the data, particularly the customer-usage data, need to be protected, archived, sanitized, or destroyed according to the varying privacy rules of the various states. Many utilities have not yet made the information-governance-related organizational adjustments required to meet these new data challenges, and that increases the chances of data misclassification, loss, or theft.

One way in which some organizations in the electric and other sectors have prepared themselves to deal more effectively with the vast amounts of data entering the enterprise has been to appoint a chief privacy officer (CPO). The CPO is typically charged with, among other duties, ensuring that all data that have federal, state, or industry-based data protection requirements be classified, monitored, maintained, and ultimately archived or destroyed according to the relevant privacy rules or the needs of the company.

Cybersecurity professionals can manage technical and procedural controls to protect data, but before those controls are selected and implemented, privacy and compliance leaders need to identify requirements, and then set and communicate the rules. There are lessons to be learned and leveraged from other data-intensive industries, such as the financial service industry's effective use of the PCI-DSS standard mentioned earlier, that helps reduce fraud by better protecting sensitive customer information

Supply Chain and Partners. Software, data, and almost everything else that helps utilities function come from suppliers outside the organization. In a perfect world, utilities would have cybersecurity requirements baked into their sourcing procedures and documents, and would demand and achieve minimum levels of security functionality when procuring all applicable systems and components. However, in many cases, including in control systems, certain types of security functionality are not available. There is a certain chicken-or-egg aspect to this, as the suppliers state that until recently their utility customers have not asked for security functionality, and the utilities say they have no choice but to procure the security technology that is available from the market. This stalemate is beginning to shift, but it is a slow process.

Communications Gear. In the current version of NERC's standards on "Critical Cyber Asset Identification," NERC tells utilities how to identify the assets that should be protected by NERC-CIP-defined controls.[20] These are typically large generators, high-voltage transmission systems and certain control centers, and the cyber systems that support them. The wireless mesh and cellular networks used as the communications paths for Smart Meters and meter data heading toward utilities, as well as for utility-control signals back to the meter networks, however, are currently considered distribution assets and therefore are not governed by NERC. Fortunately, since much of this equipment is provided by suppliers to the telecommunications market, it often includes built-in security requirements.

One of the industry organizations driving better security behavior is CTIA–The Wireless Association.[21] CTIA's cybersecurity working group identifies best practices in mobile telephony[22] and ensures they are communicated to all members and other ecosystem members. This working group could prove an example for other sectors, including the electric-power sector.

Operational Technology. While many people associate cybersecurity with anti-virus software on personal computers and firewalls for network security in corporate IT settings, it is the cyber systems that support the equipment that makes, manages, and moves electricity that is now perhaps the most in need of enhanced protections. Operational Technology encompasses a few families of systems, of which the two most common are known as SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems). These systems, designed decades ago with the assumption that the only personnel touching these machines would be authorized utility personnel or contractors, are ill-equipped for the highly networked world in which they now increasingly find themselves. While some suppliers are beginning to add security capabilities to their offerings, the process has been slow, further delayed by the fact that the normal replacement cycle of this equipment can be 20 years or more.

Physical Systems. Long before the arrival of Smart Grid technologies, utilities have been protecting substations, generation facilities, and control centers with physical controls. These include fences, door locks, security cameras, and in some cases, security guards. However, in many discussions about cybersecurity spending, someone will invariably point out the ease with which an attacker could do physical damage by firing a rifle or hurling a brick at a transformer or related exposed equipment. This is particularly the case in urban environments, where sensitive utility equipment is often surprisingly close to roads or pedestrian walkways. In rural environments, substations or transmission line towers can be hundreds of miles away from the utility charged with operating and protecting them. Utilities, therefore, use a combination of walls, fences, video cameras, motion detectors, lock systems, and other access-control methods to keep their physical assets as safe as practically possible.

Due to a widespread lack of awareness of cyber risks, employees can inadvertently cause substantial harm to utility systems or expose sensitive data.

Employees. Depending on their seniority and specialization, utility employees and contractors often have authorization to access sensitive networks, systems, and data. Since they begin with such a big head start with log-in IDs, passwords, and, depending on their position, authorization to access important systems and data, attacks by disgruntled employees or other insiders have to be considered among the most serious sources of cyber risk that utilities face. And for cost control and other reasons, utilities, as do many industries, often have to take personnel actions that can turn some of their employees against them. Of course, despite normally rigorous screening processes, hostile nation-states can also place operatives inside utilities as employees or contractors. There are, however, technological and process-based solutions to help mitigate insider threat risks, for example, limiting high-level access to a minimum number of employees.[23]

A second category of employee-related risk, not unique to the sector, is a general lack of awareness of cyber risks. Employees with no malicious intent can inadvertently cause substantial harm to utility systems or expose sensitive data. Well-known examples include clicking on links in e-mails that infect computers with malware, and the casual use of USB drives that can transmit malware to IT and OT systems.

Diverse and Varied Threats

As stated earlier, utilities should not dwell on individual adversaries. However, to the greatest extent possible, the U.S. must stay abreast of all of them. There would be no reason to worry about vulnerabilities were there not someone or some group interested in taking advantage of them to cause harm of one type or another. This section examines four categories of attackers: (1) nation-states, (2) criminal organizations, (3) terrorists, and (4) the most recent and unpredictable type known as hacktivists. Each has different motivations and capabilities, and therefore each presents different challenges to those charged with defending utilities and the power grid.

Nation-States. While it varies depending on the country in question, this threat source has the potential to finance the largest, most technically advanced, and persistent cyber-attack operations. There have already been several well-documented examples of nation-on-nation attacks that included the targeting of government and other websites as preludes to kinetic war, as was the case with the Russian attack on Georgia in 2008.[24] Prior to that episode, Russia also mounted large-scale cyber attacks on Estonia and its websites in 2007.[25] More recently comes acknowledgement of U.S. involvement in the sophisticated Stuxnet attacks that attempted to slow Iranian uranium-enrichment activities; Iran's involvement in distributed denial-of-service (DDOS) attacks on U.S. financial companies, which flood websites and applications with so much traffic that they can no longer function properly; and what appears to be Chinese targeting and penetration of a great many of the largest and most important U.S. companies.

Criminal Organizations. This element can range from lone actors with modest means to large and well-financed organizations that have advanced extortion, data theft, and other types of nefarious cyber activity to a high art. While no figures are available for the electric sector only, it is estimated that cybercrime could cost U.S. companies as much as $250 billion a year,[26] and there are documented cases of criminals attempting to extort money from utilities in return for not disabling power systems.[27]

Terrorists. Former FBI Director Robert S. Mueller has warned that terrorist groups are recruiting hackers in order to add cyber-attack capabilities to their repertoire.[28] While this is still a relatively recent threat category, one instance occurred in 2012 when the military wing of Hamas launched coordinated cyber attacks against U.S. financial institutions, said to be a reprisal for a supposedly anti-Islam film released by the controversial American pastor Terry Jones.[29] While other actors tend to stay within certain bounds due to fear of retaliation in some form, many terrorists do not share this concern. Instead of stealing money, engaging in espionage, or making political statements, terrorists tend to be most interested in catastrophic attacks that kill and disrupt their targets to the maximum extent.

Hacktivists. The best-known groups—Anonymous, Ghost Shell, and LulzSec—have confounded national defense and law enforcement officials with their fickle target selections. One week they are hacking one company or government agency for a perceived grievance, the next week they are attacking other countries and companies for entirely different reasons. The sophistication of their attacks ranges widely depending on the composition of the highly secretive, loosely knit, and geographically dispersed participants. Though they have demonstrated the potential to do real damage, hacktivists are generally viewed as less dangerous than hostile nation-states or large criminal gangs.

Managing Cyber Risks to Grid

These days, monitoring and managing cyber risks for one company in any industry is a difficult job. When considering the thousands of small, medium-sized, and large companies, some with assets and networks spanning many states, and all of which play an interconnected role in operating their section of the national grid infrastructure, it is an understatement to call it a complex and formidable challenge. Following is an overview of some of the roles and responsibilities involved.

Who Manages What. No one person or agency can manage the U.S. electric grid, which in the continental U.S. consists of three separate regional grid systems, one each for the east, west, and Texas. Everyone agrees that there is no way to reduce risks in any category, including electric-sector cybersecurity, to zero. Risk management is about being fully aware of the presence and characteristics of certain types of risk that face one's enterprise (or country) and taking steps necessary to reduce the chance of significant damage to a level in line with senior leadership's requirement and expectations. There are, however, several key actors:

The Chief Risk Officer (CRO). While CEOs ultimately own responsibility for risk in the companies they lead, in most large U.S. electric utilities it is common to find a position called chief risk officer (CRO), charged with keeping several types of risk in check. They are also tasked with regularly communicating the utility's status in each to the organization's top senior executive, often referred to as the C-Suite, and the board of directors. Typical risk categories monitored by CROs include: economic, storm and fire, supply chain, and regulatory. Yet one type of risk is typically excluded from the CRO's portfolio—cybersecurity.

Until news of Stuxnet's approach and OT impact began reaching utility executives in mid-2010, it was not clear that cybersecurity attacks could be a strategic concern for utility operations. Suddenly there existed a proof of concept and blueprint for cyber attacks that could breach IT security controls and reach and cause kinetic effects on operational systems. At that moment, a whole new level of perceived risk was born.

The Chief Information Officer (CIO). In most utilities a look at the organizational chart reveals that senior management still considers the cybersecurity threat to be primarily a low-level threat, principally a nuisance to IT systems. How is this assertion supported? The most senior person with the word "security" or "cybersecurity" in his title is a manager or a director who can be found one or two levels below the CIO on the IT side of the business. The CIO is then expected to be the translator of highly technical cybersecurity issues and terms on behalf of the C-Suite and board of directors. This arrangement is suboptimal for several reasons:

- Many utilities have a stove-piped organizational culture where IT and OT are managed separately, and operational personnel are unlikely to respond to security policy directives originating in IT.

- Most CEOs and boards rarely come in contact with personnel at the managerial or directorial level, so in some utilities it is common for them not to have any direct interaction with the senior security professional.

- Such a structure lacks a company-wide view of all large systems, networks, and end points necessary to manage cyber risk and prioritize actions from an integrated cross-enterprise perspective. In some domains this desirable holistic view is referred as a common operating picture (COP), and it cannot be achieved by utilities that are organized as described.

The Typical Utility Culture and Structure

Whether it is because their product is so essential to the livelihood and well-being of so many, or because they are dealing with machinery that can kill or injure their employees, utility companies generally have conservative cultures. Based on their consistently high level of performance and low rates of outages, it seems that conservatism has served them and their customers well. However, that same trait means that even when confronted with new technologies, business models, and threats, these change-averse organizations are slow to adapt.

There may be no truly typical utility; they come in many different sizes and with a variety of ownership models. These include: shareholder-owned, cooperatively owned, and government-owned utilities, which include federal, state, and municipal owners. The vast majority of customers are, however, served by shareholder-owned utilities.

Commonly known as IOUs (Investor Owned Utilities), these companies are structured just like their publicly owned peers in other industries. At the top are a CEO and a board of directors. Reporting to the CEO is a small group of C-level executive company officers, including a chief financial officer (CFO), a chief operating officer (COO), a chief information officer (CIO), and a chief risk officer (CRO). Depending on the size, there will also be various vice presidents running lines of business, such as generation, transmission, or customer operations. Notably, the CRO rarely has cybersecurity in the portfolio of risks that he manages.

Cybersecurity leadership functions most often fall to the CIO, typically positioned one or two levels below the CEO and charged with managing the IT side of the house. The CIO is often also responsible for cybersecurity and NERC-CIP compliance. This works well enough for the parts of cybersecurity and the CIPs that are related to IT; but it is a challenge when the CIO reaches over to OT managers. Working below the CIO will be one or several employees whose title will include the word "cybersecurity" or "security," but they have two strikes against them. First, they are seen as IT professionals by OT personnel, and therefore are not well known or trusted around operational systems. Second, they are generally too low in terms of rank to overcome organizational resistance, or to brief the CEO or board of directors.

These organizational and cultural barriers are being overcome at some utilities that are appointing more senior security leaders, who sometimes do not have to report to the CIO. But unlike financial services and telecommunications companies that have been grappling with cybersecurity threats for decades, and where it is common to find chief security officers (CSOs) or chief information security officers (CISOs), the number of large utilities with true CSOs or CISOs is still extremely low.

Of course, each utility is different and a few exemplar organizations have overcome these obstacles in one way or another, including those that have CIOs who are truly empowered to promulgate cybersecurity policy enterprise-wide, as well as a handful that have true chief security officers (CSOs), chief information security officers (CISOs), or vice presidents of security who have authority to do the same. Utilities so configured, however, are few and far between.

Information Sharing. Put simply, the term "information sharing" in the context of grid cybersecurity refers to government-to-industry, or industry-to-industry, transfers of time-sensitive knowledge related to emerging attacks or recently discovered vulnerabilities in utility cyber systems, as well as strategies to mitigate them.

When it comes to learning about new vulnerabilities and emerging threats, utilities are not alone. The Department of Homeland Security's (DHS's) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), combined with DHS's Control Systems Security Program (CSSP), has established an approach for improving the security posture of control systems within the nation's critical infrastructure. The CSSP also assists control systems vendors and asset owners and operators in identifying security vulnerabilities and developing measures to strengthen their security posture and reduce risk. The Electricity Sector Information

Sharing and Analysis Center (ES-ISAC) also performs related functions, though they are not overseen by DHS.

Information sharing itself, of course, carries its own risks. This was made clear by two recent events:

- In 2012, electric-sector security company Digital Bond released information on control-systems vulnerabilities, which it had discovered, to the general public, along with exploit codes that it developed to take advantage of the vulnerabilities.[30]

- In March 2013, NIST's national vulnerability database was itself found to be infected with malware and had to be shut down for further analysis.[31]

Such examples show the need for properly constructed information-sharing systems. Information sharing is a valuable resource for identifying threats and vulnerability information, but, if done incorrectly, it can give away what U.S. organizations know, and help hackers shift their efforts. There are also privacy concerns regarding the kind of information being shared, but these concerns can be mitigated through clear explanations of what type of information is being shared, and with careful oversight.

Pointing a way forward, The Heritage Foundation has articulated four general principles that, if they can be implemented soon and fully, will resolve most of the current information-sharing impasses in this and other sectors:

1. Congress should remove barriers to voluntary private-sector sharing. Currently, legal ambiguities impede greater collaboration and sharing of information.

2. Those entities that share information about cyber threats, vulnerabilities, and breaches should have legal protection.

3. Information that is shared must be exempted from Freedom of Information Act (FOIA) requests and use by regulators.

4. The government must be compelled to share relevant cybersecurity information and intelligence with the private sector much more quickly and completely than it does currently.[32]

Security Situational Awareness. How do utilities, or any other companies, know when they are being attacked by hackers? Until recently, the most accurate answer for many would have been: They do not know.

There are now several categories of mature cybersecurity technologies that utilities can use to monitor their IT and OT systems, to analyze whether their systems are working properly, have become infected with malware, are being probed, or are under direct attack at that moment and in danger of being shut down or otherwise impacted. These include:

- *Network and application firewalls.* These allow network traffic through approved ports and predefined application access while ostensibly blocking everything else. This is an oversimplification for brevity's sake, but the basic concept is that they keep the bad stuff (such as traffic from banned ISPs, IP addresses, and websites) and bad people (unauthorized users) out, and let the good stuff in. Firewalls are what are used to segment networks into zones to make it harder for hackers who gain access to one part of a network to reach other parts. Firewalls also keep records of their activities in log files that can be analyzed for patterns that could highlight trouble.

- *Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs).* In some ways similar to a firewall, an IDS looks for particular patterns or signatures, and therefore must be kept up-to-date if it is to detect the latest versions of evolving automated attacks. An IPS goes one step further by blocking traffic that meets blacklisted criteria.

- *Security Incident and Event Management (SIEM) Systems.* These can tap into many different types of systems (such as servers, routers, databases, or SCADA), read their log files, and subject them to rapid and sophisticated analysis to correlate patterns, reduce the number of potential issues to a manageable size, and present an almost real-time dashboard view of the organization's security posture.

Most utilities implement some or all of these technologies for their networks and systems, either themselves or through third-party security services providers. The variables that determine the quality of the security include how well defensive systems are configured and how closely they are monitored by qualified personnel. These tool categories were all developed for use in IT environments, and, while a few vendors' offerings can work in OT environments, most are incompatible with the demanding network latency and system overhead limitations found there.

Of course, there is also a non-technical aspect to security—situational awareness, having to do with people. When one knows how systems and processes work and can recognize when they are running properly, it is easier to detect deviations from the norm.

Cybersecurity Economics. How do utilities fund cybersecurity activities? One thing they have in common with companies in every other sector is that security expenditures are always a cost; they are never about making money. Furthermore, while factoring security requirements into large projects will almost always entail some additional up-front costs, adding security after the fact to legacy systems is guaranteed to both substantially increase expenses and potentially restrict functionality.

Therefore, utilities that invest in cybersecurity proactively, rather than after the fact, spend less money overall. Here are two of the ways they save:

1. *Breach costs.* Numerous independent studies have tallied the costs of security and privacy breaches and have arrived at figures that get most utilities' attention. In data security breaches affecting customers, for example, the average cost per customer record lost was $194, and the average total cost per incident in 2011 was $5.5 million.[33]

2. *NERC CIP violations.* Utilities owning assets that meet the CIP criteria are subjected to recurring compliance audits, with the penalty for failure, at the auditors' discretion, as high as $1 million per day of noncompliance. A look at the actual fines levied reveals that most are in the range of several tens to several hundreds of thousands of dollars.[34] These fines represent a financial impact even when *no* breach occurs, as the utilities must already invest heavily to fund their dedicated CIP-compliance teams. At the larger utilities, these can total 20 to 40 full-time personnel, costing several millions of dollars per year.

In order to avoid the costs above, utilities include requests for security expenditures in their rate cases to the commissioners of the state or states in which they operate. Essentially, these are business case arguments asking for funding for certain tasks, making the connection to reliability, and while the funding is often approved, it is sometimes at a reduced level. In fact, there have been cases where citizens groups have petitioned to block or limit the amount approved for security in rate cases on the grounds that the requested security expenditures are supposedly excessive or do not, in their opinion, deliver any value to them.[35]

Security expenditures are always a cost; they are never about making money.

So, while some utilities are criticized for responding slowly to the new, more dangerous security landscape, even when they want to make substantial improvements, they are not necessarily masters of their own destiny. Also, as Appendix C summarizes, some types of utilities, including large IOUs, will likely come under increasing economic pressure as new challenges to their business models emerge, which will create a climate that will likely make increased cybersecurity expenditures even harder to justify.

Practicing to Better Prepare for Real Incidents. There was a time when many believed that having security firewalls in place provided adequate protection of their networks and therefore all the systems within. That illusion of near-complete protection was largely debunked with the arrival of Web applications, all of which had to pass through certain firewall ports in order to be useful to customers and employees alike. But, while for some the perception of invincibility still exists, the daily drumbeat of breaches of organizations of all kinds is waking most people up to the fact that no company or government organization is invulnerable, no matter how robust its cyber defenses seem to be.

So the challenge facing utility executives has become how they should prepare and how they want their team to respond when their cyber systems are breached. Following are a few representative questions with which utilities are grappling:

- When we have a breach and it appears we may have lost a few hundred thousand, or even a million, customer records, which departments will respond?

- Is this a crime or a mistake? It is too early to know, so how should we characterize this for law enforcement?

- How will we present events and our actions to the media, especially since we are not sure yet about how the breach happened?

- What is the best, safest, and most responsible approach our legal department should take?

- How do we best communicate with our customers, both those affected and those not?

- What should we be prepared to offer our customers whose personally identifiable information (PII) might have been exposed?

- How will we determine how the breach occurred? Do we need to bring in a third-party forensics team? If there is a gap in our technical controls, will our security personnel know how to close it?

Data loss events are one of the more common types of breaches and are usually the result of an insecure business system or process on the IT side, including the loss or theft of a mobile device. Training and preparation for breaches or other cyber incidents that could impact operational equipment are important steps to take, will potentially involve a variety of different personnel, and could involve cooperation with regional grid operators.

Along these lines, NERC CIPs include requirements for utilities that own critical cyber assets to develop, maintain, and exercise cyber-incident reporting, response, and recovery. NERC says these plans need to be tested at least annually, and allows that acceptable forms of testing range from simple paper drills to full-blown operational exercises.

In the same spirit, but on a larger scale, NERC conducts an exercise called GridEx that involves North American bulk-power-system owners and operators, as well as appropriate government agencies. In NERC's words, the objective of the GridEx exercise is to

> test NERC's and the electricity industry's crisis response plans, and validate current readiness in response to a cyber incident. The exercise also serves as an opportunity to enhance collaboration and strengthen industry security processes and capabilities.[36]

It is clear is that, while utility executives can hope that their staff is spending money on the right cybersecurity protective measures, they can begin to buy themselves some peace of mind by ensuring that their entire team is prepared, and practicing, to do the best job possible when a breach occurs.

Government and Industry Guidance

While many questions and much work remain, a number of government and industry entities have compiled guidance that can be used as a basis to plan and enhance utility security. The first and possibly best and most complete document related to securing modernized grid systems is NIST's Inter-agency Report 7628, *Guidelines for Smart Grid Cyber Security*. Released in 2010 in three volumes comprising nearly 600 pages, the "NISTIR 7628," as it is known, remains the most definitive work on the subject.[37] In 2012, NIST released an adjoining assessment guide; the primary document is under revision at the time of this writing.[38]

There are also a number of other guides, most intended for utilities themselves, that seek to make the sometimes overwhelming challenges of security more tractable.

Altogether, these resources, listed in Appendix D, deliver some extremely helpful information for utilities seeking direction in securing both their IT and their OT systems and networks. Other helpful resources include GAO reports on successes and failures in grid security, particularly the performance of the Department of Energy, FERC, and NERC. The Department of Energy has also published security roadmaps to help utilities, suppliers, and integrators better understand how to secure OT systems.

A More Secure Electric Grid

The U.S. electric grid is part of critical national infrastructure; in fact, as none of the other sectors can operate without it, it is arguably the most critical of all. At the time of this writing, there is a tremendous amount of good work being done to advance the state of grid security by members of industry, government, academia, and, especially, by professionals in the utilities themselves. Yet for reasons described earlier, many people believe that the U.S. grid is still inadequately protected against increasingly powerful and persistent cyber threats.

Part of the security problem can be attributed to the complexity of the grid itself, as well as to the overwhelmingly complex software and communications systems that help manage it. For too long, electric utilities, like other critical infrastructure providers, have accepted ever-increasing technological complexity as the natural state of things. It is very hard, however, to secure a system one can barely understand. Therefore, utilities should reconsider their acceptance of complexity, and consider moving to a position where simplicity becomes a value to be pursued. Over the coming years, utilities should be guided, through collaboration with government, to streamline and simplify their IT, OT, and communications to the greatest extent possible.

Other recommendations touch upon organizational issues, such as updating the governance model and organization chart to better meet the challenges stemming from changes in how systems are connected and the ever increasing capabilities of adversaries.

The biggest challenge, though, may be the profound lack of rudimentary tools and metrics to describe the levels of security capabilities at individual utilities or across portions of the grid. Absent a mutually agreed way of characterizing relative preparedness strengths or weaknesses, neither the regulators nor the utilities have a means for establishing a baseline, and without a baseline, it is impossible to build road maps to desired, higher-functioning states. Therefore, the first recommendation is about security metrics. Though much of the work to be done rests in the hands of the private sector, there are key steps Congress, the Administration, and states can take to help ensure the security of the electric grid. These include:

Enabling effective information sharing by removing legal ambiguities to sharing, providing strong protections for sharers, and establishing a clear mechanism for sharing. Entities that share cybersecurity information need certain protections. These protections include exempting all shared information from FOIA requests and regulatory use, and providing information sharers with strong liability protection. Effective information sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership established for this purpose, as well as through already existing ISACs. Information sharing must work in both directions so that utilities and government are receiving the latest in cybersecurity threat and vulnerability information from each other.[39]

Working collaboratively with utilities to encourage cybersecurity performance measurement. The capacity to improve the security stance of utilities begins with a common language to describe the ways in which they are currently protected against current threats.

Improvements are gradually being made to the U.S. electric grid through the normal acquisitions process.

Metrics should not be focused on technologies and system-level information, while such may well be included. The types of metrics that are most needed are those that measure cybersecurity awareness throughout an organization as well as the effectiveness of clearly defined responsibilities and programs. Measurements for presence of malware, client and trusted-user susceptibility to common attack types, and presence of security considerations as documented in strategic plans, contracts, component solicitation, supply-chain validation, and executive-level tracking are examples.

This effort should also be undertaken with the goal of providing a common language and set of expectations for regulators and utilities, with an emphasis on performance over compliance. The Administration should realize that time will allow these measures to develop into a set of consistent best practices and measures, ultimately leading to applicable maturity models, but those should be seen as evolutions of this initial effort; given the immaturity of security in this space, there needs to first be agreement on what is common, what is expected, what is desired, and what is possible.

To that end, the Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) is a good starting point. As it informs the NIST CSF, and as it is improved in subsequent versions, so will utilities' ability to selfassess and map out better positions to improve as well. The Administration should engage with and support utilities as they gradually improve their cybersecurity.

Realizing that the electric grid is already making strides to improve its cybersecurity. Over time, utilities will become more secure as older, insecure systems are retired and newer, more secure systems take their place. Congress and executive and regulatory agencies should realize that improvements are gradually being made to the U.S. electric grid through the normal acquisitions process.

In those cases where there is a long lag time, or little opportunity to update critical systems, utilities should develop strategies to reduce risk and increase visibility through mitigating controls, newer technologies, and interfaces that broker relationships between these systems and the rest of the network, trusted or untrusted. In these cases, the executive branch should avoid costly, mandatory regulations that will require specific fixes and instead collaborate with industry and encourage its members to:

- *Create* an inventory of all systems, networks, applications, and databases, focusing on a reduction of redundancy, unnecessary connection, and elimination of any unneeded points of access;

- *Create* a governance and change-management plan that will ensure that the systems they plan to continue using are configured properly for security, patched promptly, and accessible only by those who have a need to use them; and

- Even though they may not be able to secure all legacy systems, especially in OT, to their satisfaction, *ensure* that any new systems purchased and deployed comply with the utilities' security policies.

Encouraging private-sector cyber awareness, education, and training by working with industry to develop dynamic education programs. While the media and pundits speak out frequently, and often greatly hype, about various threat sources—whether nation-states, terrorist groups, hacktivists, or criminals—there is little that is of material benefit to utilities on that vague level of understanding. On the other hand, feel-good security measures only lead to a false sense of security. Instead of either extreme, there are things that utilities should be hearing and measures they should be taking to make themselves much tougher targets to breach. In almost all published breaches, the breach inception occurs through a variety of relatively simple causes rooted in a lack of consistency, awareness, and investment.

Since many if not most IT breaches result from uninformed human behaviors, like clicking on benign-looking but malicious links in e-mails, the U.S. should pursue widespread cybersecurity education and training. This should be accomplished in a number of ways, including through meaningful and consistent, but not hyped, warnings and briefings from government officials. Additionally, the Administration should direct DHS and regulators to work with industry groups in encouraging and updating cybersecurity education policies that cover both general cybersecurity hygiene as well industry-specific policies. Ideally, this education will be formulated by the private sector itself. Specifically for the grid, utilities should create awareness programs that will help each employee to better understand his responsibility in maintaining the utilities' own systems and corporate networks.

Utilities should train their employees to be more wary of problems through regular interaction with security content, substituting traditional long-form education with more interactive training, exercises, and testing. The government can and should provide assistance to utilities in building this kind of cyber awareness.

Recognizing and reinforcing the crucial role that states play in oversight of utility cybersecurity within their borders since NERC CIPs cover only a small percentage of overall grid assets. States have purview over the lion's share of grid assets, and while state utility commissions will likely never match the subject-matter expertise or technical acumen of the electric utilities they regulate, they must improve their understanding of cybersecurity basics at least enough to perform their oversight role more effectively. The mismatch seen in many states today, where commissions have no choice but to take utilities at their word that they are prioritizing cybersecurity spending and activities appropriately, is not healthy for either side nor is it likely to provide best results for their many and various customers. For state commissions, the best place to start is the National Association of Regulatory Commissioners Cybersecurity Guidelines for State Commissions, which is at once a concise primer and a source of targeted questions useful for sparking informative two-way conversations between utilities and state commissions on cybersecurity.

Incentivizing security enhancements. Suppliers of IT and particularly OT technologies to utilities need to design and deliver systems with security capabilities that are appropriate for the times. In order to motivate this private-market behavior, utilities need to specify, purchase, and field systems with security as a baseline criterion, so that security will organically improve as older systems fail or are retired.

To encourage this behavior, the Administration should develop, refine, and select from among the candidates incentive categories generated as part of the NIST CSF effort. In particular, the Administration should work with Congress to promote:

- *Cybersecurity insurance* for utilities provided by private insurers,
- *Strong liability limitations* for information sharing and cybersecurity actions,
- *Streamlined regulations,*
- *Stronger support* for utilities' requests for additional cybersecurity investments during rate-case proceedings, and
- *Cybersecurity research* by the private sector and government.

Fostering good behavior throughout the electric power ecosystem by assisting in the development of a viable liability system for cybersecurity. Neither federal nor state governments are agile enough to offer detailed, prescriptive guidance to utilities on how they should secure themselves. This is a fact and a natural consequence of a robust deliberative legislative and regulatory process.

The potential for losses as a result of a cybersecurity failure can however be used to push utilities to seek reasonable levels of cybersecurity. Instead of mandating specific actions that will consistently change as threats and technologies change, the U.S. should motivate proper security by allowing companies to be civilly liable for lax or improper security rigor in cases where breaches and difficulties are exposed. On the other hand, there may be a place for liability limits, such as through the SAFETY Act, in order to prevent a chill on cybersecurity innovation. Congress should investigate more fully if and where these limits might be needed.

Currently, boards of directors for utilities are often unaware of and unconcerned with the details of their utilities' cybersecurity and risk. However, being liable for cyber breaches and having insurance premiums based on a utility's security level can change this dynamic and force boards to consider the real reputational and financial risks of lax cybersecurity. While every organization and utility will respond differently to understanding and mitigating its cyber risks, utilities with engaged boards of directors, who have a clear Common Operating Picture of their utilities' cybersecurity and cyber risk, will likely handle cyber challenges in more thoughtful and meaningful ways. Such actions will demonstrate to federal and state regulators and all other stakeholders (including Congress) that the utility is taking concrete steps to improve its cybersecurity operations and awareness.

Going Forward

There is much to learn from the modernization that has been undertaken, and in fact, will continue, in different industries. Similarly, there are already good examples and precedents for achieving higher levels of security at U.S. electric utilities. No new technologies need be created or deployed to get the grid to a better, more secure place. Rather, a few, straightforward strategies, promoted by senior government leadership and adopted by utilities, have the potential to produce markedly better results. If the outcomes of these recommendations can be achieved, in full or even in part, the U.S. grid, and all the other critical infrastructures that depend on it, will attain a demonstrably improved security position. And the United States will have reduced this currently substantial category of risk to a level that is significantly more manageable.

Appendix A:

Security Terms to Know

Knowing these definitions will not make you an instant cybersecurity expert, but should help to remove some of the mystery from a topic that is often considered too technical and esoteric for generalists to understand:

- **Access control:** methods to ensure that only authorized persons (or machines) are allowed to access a system or network.

- **Application security:** using secure programming techniques or application scanning tools to identify and remove vulnerabilities in software that could be exploited by attackers.

- **Attack surface:** the total number of pathways into a network or system that an attacker could attempt to use. Defenders have to understand attack surfaces of their systems in order to reduce them as much as possible and defend what is left.

- **Data security:** ensuring that sensitive data is only accessible by approved systems and users.

- **Defense in depth:** an organization should not count on any single layer of cybersecurity to protect the system from all threat types; rather, the organization should deploy multiple rings of different types of defense—defense in depth—to make it more likely that an attacker will be thwarted by at least one of them.

- **Encryption and cryptography:** scrambling data using a "key" algorithm before moving it across a network. Also refers to scrambling data at rest, as in when they are saved on a storage device.

- **Patch management:** software has become so complicated that vulnerabilities continually arise out of that complexity. When they do, often thanks to hackers, testers, and analysts from all walks of life, the company that created the software will often create a "patch" to fix it. Unfortunately, security patches are also software, and often create as many vulnerabilities as they resolve. This pattern repeats itself endlessly.

- **Penetration (or Pen) Testing:** instructing one's own personnel, or third parties, to attempt to break into one's own networks and systems. When they are successful, their job is to document how they breached the system, and recommend steps for closing off those routes.

- **Shodan:** a search engine that reveals all Internet-connected devices, including a great many from the energy sector, including generators and other OT equipment.

- **Zero-day attacks:** refers to existing vulnerabilities that have yet to become official "known vulnerabilities." They are particularly valuable and can be sold by the person or organization that discovers them, as they can be assumed to be present and unpatched in every deployed version of that operating system or application.

Appendix B:

NERC CIPs: Past, Present, and Future

Version 1 of the NERC CIPs had its origin in 2005 with the passage of the Federal Power Act; subsequent versions have largely been responses to FERC's Order 706, the "Mandatory Reliability Standards for Critical Infrastructure Protection" in 2008. Prior to the CIPs, FERC was responsible for monitoring and ensuring reliability but did not have a cybersecurity function. The first version omitted several cybersecurity basics, such as pen testing, encryption, and software security. Subsequent versions address security controls more comprehensively.

Versions 1, 2, and 3 of the CIPs gave utilities leeway in developing their own custom risk-management process to determine which of their generators, transmission assets, or control centers should be considered critical and, therefore, subject to mandatory CIP controls and audits. Many utilities erred on the side of excluding assets in their risk-management processes.

With version 4, approved by FERC in 2012, NERC has provided "bright line criteria," which remove wiggle room by giving utilities cutoff points for determining which systems are critical and must comply with the CIPs. Version 5, passed by NERC in 2012 and awaiting approval or rejection by FERC at the time of this writing, will encompass many more systems by requiring utilities to categorize all their bulk assets as high-impact, medium-impact, or low-impact. While there is still a large amount of uncertainty about how this will play out, NERC will be auditing more of the bulk electric system, and the audits also mean much new work for utilities, most of which already feel overburdened by CIP compliance costs and activities.

Lastly, a largely one-sided debate rages in the community claiming that compliance does not equal security, and that the CIPs are distracting utilities from more effective security work. On the other hand, many utility security personnel who have been working the CIP program since version 1 report that their companies are more aware and more secure at this point than they would have been without the mandatory program. Regardless, the CIPs will remain for the foreseeable future, and the utilities' challenge is to do an increasingly good and efficient job of achieving and demonstrating compliance, while keeping themselves as secure as possible.

Appendix C:

Economic and Business Challenges to IOUs May Threaten Cybersecurity Investments

In a recent report on potentially disruptive threats to the industry, the U.S. electric utility advocacy group Edison Electric Institute (EEI) reviewed current trends in the adoption of distributed energy resources (DER) by consumers and warned IOUs that their timeworn business model may not be sustainable much longer.

More specifically, EEI laid out the economic challenges:

> [The] headwinds facing the sector are significant. Concerns start with the anemic electricity demand, which has been primarily impacted by the overall economic climate but also impacted by demand-side efficiency programs and the emergence of DER. Next, there is the need to deploy capital investment at almost twice the rate of depreciation to enhance the grid and address various regulatory mandates. Soft electricity demand plus increasing capital investment lead to rate increase needs and the investment uncertainty created by a future active rate case calendar. While sell side analysts are expecting EPS [earnings per share] growth of 4 percent to 7 percent overall for the regulated sector, this is likely to be quite challenging. If investor expectations are not realized, a wholesale reevaluation of the sector is likely to occur.... [Also, this] set of dynamics can become a vicious cycle...that, in the worst-case scenario, would leave fewer customers remaining to support the costs of a large embedded infrastructure system.[40]

These types of alarms have been sounded by the energy sector, as well as by the journalists that cover it, for a little while, but when the normally conservative EEI begins relaying messages this cautionary, it is a signal to many that large changes may be coming to the sector sooner than previously anticipated. This is concerning from a cybersecurity perspective, since companies struggling to master corporate survival challenges may be less willing to fund cybersecurity investments, even if they see them as necessary.

Appendix D:

Key Guidance Documents

A variety of information is available to companies and organizations with responsibility for cybersecurity in the electric grid. Following is some of the key guidance:

- **Edison Electric Institute, "Principles for Cyber Security and Critical Infrastructure Protection," September 9, 2010**, http://www.eei.org/Documents/cyber_security_principles.pdf (accessed November 19, 2013). This offers cybersecurity guidance for the industry in general, and the large IOUs in particular, as well as recommendations for the best ways in which the government can provide support.

- **Miles Keogh and Christina Cody, "Cybersecurity for State Regulators 2.0," The National Association of Regulatory Utility Commissioners, February 2013**, http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf (accessed November 19, 2013). This is an excellent primer to help state commissioners, most without any cybersecurity background, understand the relevant issues. It also arms commissioners with sample questions on cybersecurity policies and practice designed to elicit helpful responses.

- **National Rural Electric Cooperative Association (NRECA), "Guide to Developing a Cyber Security and Risk Mitigation Plan," 2011**, http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf (accessed November 19, 2013). Often minimally staffed and underfunded, rural utilities are responsible for electric power services for the majority of the landmass of the United States. Knowing their limitations as well as their obligations, NRECA's guide is both a primer and an instruction manual intended to help smaller utilities carry out necessary cybersecurity functions.

- **U.S. Department of Energy, "Electricity Subsector Cybersecurity Maturity Model (ES-C2M2) Program,"** http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2 (accessed November 19, 2013). This model is a first attempt to help utilities baseline their current security posture, identify gaps, and develop road maps for improvement in categories that align with their business requirements.

- **U.S. Department of Energy, "Electricity Subsector Cybersecurity: Risk Management Process," March 2012**, http://energy.gov/sites/prod/files/RMP%20Guideline%20Second%20Draft%20for%20Public%20Comment%20-%20March%202012.pdf (accessed November 19, 2013). This guideline helps translate cybersecurity tasks and priorities into a risk-management framework that fits within the larger risk-management context at a utility.

Endnotes

1. "Who's Afraid of Huawei?" *The Economist*, April 4, 2012, http://www.economist.com/node/21559922 (accessed November 7, 2013).
2. Emil Protalinski, "Senate Blocks Cybersecurity Act," ZDNet, August 2, 2012, http://www.zdnet.com/senate-blocks-cybersecurity-act-7000002051/ (accessed September 11, 2013).
3. News release, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed September 11, 2013).
4. Dan Mcwhorter, "Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators," Mandiant, February 18, 2013, https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/ (accessed September 11, 2013).
5. Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *The New York Times*, March 20, 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0 (accessed September 11, 2013).
6. Matthew J. Schwartz, "China Tied to 3-Year Hack of Defense Contractor," InformationWeek Security, May 2, 2013, http://www.informationweek.com/security/government/china-tied-to-3-year-hack-of-defense-con/240154064 (accessed September 11, 2013).
7. "Edward Snowden: Timeline," BBC, August 20, 2013, http://www.bbc.co.uk/news/world-us-canada-23768248 (accessed September 11, 2013), and James Jay Carafano, "For Conservatives, Snowden Is Hero and Horror," Heritage Foundation *Commentary*, June 27, 2013, http://www.heritage.org/research/commentary/2013/6/for-conservatives-snowden-is-hero-and-horror.
8. National Institute of Standards and Technology, "Discussion Draft of the Preliminary Cybersecurity Framework," August 28, 2013, http://nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf (accessed September 11, 2013).
9. Rhonda Schwartz, "U.S. Confirms Syrian Electronic Army Defaced Marines Website," ABC News, September 3, 2013, http://abcnews.go.com/blogs/headlines/2013/09/u-s-confirms-syrian-electronic-army-defaced-marines-com/ (accessed September 12, 2013).
10. The Energy Library, "North American Electricity Grid," 2009, http://www.theenergylibrary.com/node/647 (accessed November 7, 2013).
11. While each state has its own utility commission, one of the best places to learn about the issues the commissions face, including cybersecurity policy, is the central body in Washington, D.C., the National Association of Regulatory Utility Commissioners (NARUC), http://naruc.org/ (accessed November 7, 2013). Another good resource is the National Association of State Energy Officials (NASEO), http://www.naseo.org/ (accessed November 7, 2013).
12. In early 2013, FERC clarified and simplified the definition of BES assets to refer to "any transmission element operated at 100kV or above, and any [generation] resource connected with the grid at 100kV or higher" as well as "system elements that operate below 100kV…if they are 'necessary for the operation of the interconnected transmission network.'" Andrew Art and Ilan Gutherz, "FERC Approves New Definition of Bulk Electric System, Reserves Determination of Which Facilities Are 'Used in Local Distribution,'" Van Ness Feldman, January 2, 2013, http://www.vnf.com/news-alerts-784.html (accessed September 12, 2013).
13. Competing attribution for the origination of the term "Smart Grid" given to University of Minnesota professor and IEEE member Dr. Massoud Amin, and Andres Carvallo who was CIO of Austin Energy at the time.
14. For more information on synchrophasors, see Schweitzer Engineering Laboratories, "Synchrophasors Overview," 2013, https://www.selinc.com/synchrophasors/ (accessed September 12, 2013).
15. Infosec Island, "ICS-CERT Warns Facilities of Exposure via SHODAN," December 12, 2011, http://www.infosecisland.com/blogview/18681-ICS-CERT-Warns-Facilities-of-Exposure-via-SHODAN.html (accessed September 17, 2013).
16. National Institute of Standards and Technology, "Recommended Security Controls for Federal Information Systems and Organizations," *Special Publication* No. 800-53, May 1, 2010, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (accessed September 12, 2013), and Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology *Special Publication* No. 800-82, June 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (accessed September 12, 2013).
17. U.S. Department of Defense, "Report of the Defense Science Board Task Force on DoD Energy Strategy: 'More Flight—Less Fuel,'" February 2008, http://www.acq.osd.mil/dsb/reports/ADA477619.pdf (accessed September 12, 2013).
18. Ibid.
19. Andy Bochman and Dan Nolan, "Navy Connects to Achieve Physical, Cyber and Energy Security at Naval District Washington," The DOD Energy Blog, May 8, 2013, http://dodenergy.blogspot.com/2013/05/navy-connects-to-achieve-physical-cyber.html (accessed September 12, 2013).
20. North American Electric Reliability Corporation, "Cyber Security–Critical Cyber Asset Identification," CIP-002-3, December 16, 2009, http://www.nerc.com/files/cip-002-3.pdf (accessed September 12, 2013).

21. CTIA stands for Cellular Telecommunications & Internet Association, the name of the association until 2004. CTIA–The Wireless Association, http://www.ctia.org/ (accessed September 12, 2013).
22. Mobile telephony refers to telephone service provided to mobile phones.
23. The National Security Agency (NSA) is in the process of cutting its "system administrators by about 90 percent," according to General Keith Alexander, head of the NSA. The NSA is accelerating these measures after system administrator Edward Snowden was able to download large amounts of data and flee the U.S. Jonathan Allen, "NSA to Cut System Administrators by 90 Percent to Limit Data Access," Reuters, August 8, 2013, http://www.reuters.com/article/2013/08/09/us-usa-security-nsa-leaks-idUSBRE97801020130809 (accessed September 27, 2013).
24. John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed September 12, 2013).
25. Joy Wang, "The 2007 Estonian Cyberattacks: New Frontiers in International Conflict," On Cyber War–Freshman Seminar 43z–Internet Law, December 21, 2012, http://blogs.law.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/ (accessed September 12, 2013).
26. Peter Maass and Megha Rajagopalan, "Does Cybercrime Really Cost $1 Trillion?" *The Huffington Post*, August 1, 2012, http://www.huffingtonpost.com/2012/08/01/keith-alexander-nsa_n_1729757.html (accessed September 12, 2013).
27. Kenneth G. Brill, "Preparing for A Cyber Attack," *Forbes*, November 19, 2009, http://www.forbes.com/2009/11/19/cybersecurity-power-grid-technology-cio-network-blackout.html (accessed September 12, 2013).
28. Emil Protalinski, "FBI Warns Congress of Terrorist Hacking," ZDNet, March 8, 2012, http://www.zdnet.com/blog/security/fbi-warns-congress-of-terrorist-hacking/10601 (accessed September 12. 2013).
29. Christopher Collins, "Hamas Organization Behind Recent Cyber-Attacks on Financial Institutions," Examiner.com, March 31, 2013, http://www.examiner.com/article/hamas-organization-behind-recent-cyber-attacks-on-financial-institutions (accessed September 12, 2013).
30. Sean Gallagher, "A Valentine's Day Present for SCADA Companies: New Exploit Tools," ArsTechnica, February 9, 2012, http://arstechnica.com/business/2012/02/a-valentines-day-present-for-scada-companies-new-exploit-tools/ (accessed September 12, 2013).
31. Grant Gross, "U.S. NIST's Vulnerability Database Hacked," Computerworld, March 14, 2013, http://www.computerworld.com/s/article/9237605/U.S._NIST_s_vulnerability_database_hacked (accessed September 12, 2013).
32. Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.
33. News release, "Ponemon Study Shows the Cost of a Data Breach Continues to Increase," Ponemon Institute, January 25, 2010, http://www.ponemon.org/news-2/23 (accessed September 12, 2013).
34. NERC, "Enforcement Actions–2013," http://www.nerc.com/pa/comp/Pages/Enforcement-Actions-2013.aspx (accessed November 15, 2013).
35. Marc Lifsher, "Fight over Southern California Edison Rate Hike Heats Up," *Los Angeles Times*, July 26, 2011, http://articles.latimes.com/2011/jul/26/business/la-fi-edison-rate-hike-20110726 (accessed September 12, 2013).
36. NERC, "GridEx," 2013, http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx (accessed September 12, 2013).
37. NIST, *Introduction to NISTIR 7628: Guidelines for Smart Grid Cyber Security*, September 2010, http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (accessed November 15, 2013).
38. NIST, *Guide for Assessing the High-Level Security Requirement in NISTIR 7628*, December 20, 2011, http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/NISTIR_7628_Assessment_Guide-v0p9.pdf (accessed November 27, 2013).
39. Bucci, Rosenzweig, and Inserra, "A Congressional Guide."
40. Peter Kind, "Disruptive Challenges: Financial Implications and Strategic Responses to a Changing Retail Electric Business," Edison Electric Institute, January 2013, p. 11, http://www.eei.org/ourissues/finance/Documents/disruptivechallenges.pdf (accessed September 12, 2013).

The Heritage Foundation

214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400

heritage.org