Energy & Infrastructure Program
Energy Project

National Security Program
Homeland Security Project

Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat

A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative

February 2014

BIPARTISAN POLICY CENTER

DISCLAIMER

The findings and recommendations expressed within this report are those of the co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative. While these findings and recommendations were informed by the discussion with the advisory group listed on page 1, they do not necessarily represent the views or opinions of advisory group members or the organizations they represent.

Bipartisan Policy Center Electric Grid Cybersecurity Initiative Participants

CO-CHAIRS

General (Ret.) Michael Hayden
Principal, The Chertoff Group; former Director, CIA; former Director, NSA

Curt Hébert
Partner, Brunini, Grantham, Grower & Hewes, PLLC; former Chairman, FERC; former Chairman, Mississippi Public Service Commission

Susan Tierney
Managing Principal, Analysis Group; former Assistant Secretary for Policy, DOE; former commissioner, Massachusetts Department of Public Utilities

ADVISORY GROUP MEMBERS

Scott Aaronson
Senior Director, National Security Policy, Edison Electric Institute

Scott Baron
Director, Digital Risk and Security Governance, National Grid

Jim Burpee
President & CEO, Canadian Electricity Association

Terry Boston
President & CEO, PJM Interconnection

Robert Caldwell
Chief Cyber Security Architect, General Electric

Paul Centolella
Vice President, Analysis Group; former commissioner, Public Utilities Commission of Ohio

Roger Duncan
Research Fellow, Energy Institute, University of Texas; former General Manager, Austin Energy

Jessica Matlock
Director, Government Relations, Snohomish County Public Utility District

Jeff Nichols
Director, Information Security and Management, Sempra Energy Utilities

James Sample
Chief Information Security Officer, Pacific Gas and Electric Company

Paul Stockton
Managing Director, Sonecon; former Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

Mark Weatherford
Principal, The Chertoff Group; former Deputy Undersecretary for Cybersecurity, DHS

BPC ELECTRIC GRID CYBERSECURITY INITIATIVE STAFF

Margot Anderson
Executive Director, Energy Project

Joe Kruger
Director for Energy and Environment

Carie Lemack
Director, Homeland Security Project

Blaise Misztal
Acting Director, Foreign Policy Project

Meghan McGuinness
Associate Director for Energy and Environment

Jason Burwen
Senior Policy Analyst

Blair Beasley
Policy Analyst

Rosemarie Calabro Tully
Press Secretary, Energy

Abbey Brandon
Press Assistant

Amanda Kaster
Project Assistant

ACKNOWLEDGEMENTS

The Bipartisan Policy Center (BPC) would like to thank its funders for their strong support. We also thank advisory board members Paul Stockton of Sonecon, LLC, who drafted Chapter 5 of this report, and Paul Centolella of the Analysis Group who drafted portions of Chapters 2, 3, and 6. We are grateful for their expertise and contributions. We thank Doug Smith and Andrew Art of Van Ness Feldman, LLP for their invaluable input. We are grateful to Colleen Kelly, former policy analyst with the Energy Project, and Blake Harwood, former intern with the Homeland Security Project, for their work on the early stages of this project. In addition, we would like to thank NARUC and Commissioner Phillip Jones of the Washington Utilities and Transportation Commission for their helpful comments on a draft of this report. Special appreciation is also due to Marika Tatsutani for editing the report. Finally, we would like to acknowledge the following key staff or colleagues of advisory board members for the many contributions to this report:

Patrick Brown, Director, U.S. Affairs, Canadian Electricity Association
Chris Foster, Manager, Federal Government Relations, Pacific Gas and Electric Company
Scott King, Information Security Manager, Sempra Energy Utilities
Sean Mackay, Government Affairs, Sempra Energy

Table of Contents

List of Acronyms

AFNG	Air Force National Guard
AMI	Advanced Metering Infrastructure
BPC	Bipartisan Policy Center
CCRIC	Canadian Cyber Incident Response Centre
CEDS	Cybersecurity for Energy Delivery Systems
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CISPA	Cyber Intelligence Sharing and Protection Act
CRISP	Cybersecurity Risk Information Sharing Program
DHS	U.S. Department of Homeland Security
DOC	U.S. Department of Commerce
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
ECPA	Electronic Communications Privacy Act
EPRI	Electric Power Research Institute
ESCC	Electricity Sub-sector Coordination Council
ES-C2M2	Electricity Sector Cybersecurity Capability Maturity Model
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
GAO	Government Accountability Office
GCC	Government Coordinating Council
GICSP	Global Industrial Cyber Security Professional
GRID	Grid Reliability and Infrastructure Defense
GridEx	Grid Security Exercise
GridSecCon	Grid Security Conference
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
INPO	Institute of Nuclear Power Operations
ISAC	Information Sharing and Analysis Center
MOU	Memorandum of Understanding
NARUC	National Association of Regulatory Utility Commissioners
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NCRAL	National Cyber Risk Alert Level
NEIL	Nuclear Electric Insurance, Ltd.
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRF	National Response Framework

NSF	National Science Foundation
PSC	Public Safety Canada
PUC	Public Utility Commission
RMP	Risk Management Process
SAFETY	Support Anti-Terrorism by Fostering Effective Technologies
SCADA	Supervisory Control and Data Acquisition
SnoPUD	Snohomish County Public Utility District
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TRIA	Terrorism Risk Insurance Act
UCG	Unified Coordination Group
US-CERT	U.S. Computer Emergency Readiness Team

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Summary of Findings and Recommendations

Introduction

Protecting the nation's electricity grid from cyber attacks is a critical national security issue. Evidence collected by the U.S. Department of Homeland Security (DHS) suggests that cyber attacks on key energy infrastructure—and on the electricity system in particular—are increasing, both in frequency and sophistication. These trends are alarming because the potential consequences of a successful large-scale cyber attack—or combined cyber and physical attack—on the electric power sector are difficult to overstate. As previous grid failures, including the multiday Northeast blackout of 2003, have shown, any event that causes prolonged power outages over a large area would not only be extremely costly, it would wreak havoc on millions of people's daily lives and could profoundly disrupt the delivery of essential services, including communications, food, water, health care, and emergency response. Moreover, cyber threats, unlike traditional threats to electric grid reliability such as extreme weather, are less predictable in their timing and more difficult to anticipate and address. A cyber attack could come from many sources and—given the size and complexity of the North American electric grid—could target many potential vulnerabilities. For this reason, experts agree that the risk of a successful attack is significant, and that the system and its operators must be prepared to contain and minimize the consequences.

Current efforts to provide for electric grid cybersecurity are dispersed and involve numerous federal, state, and local agencies. In some ways, the electric sector is in a stronger position than other sectors to address cyber threats because it already has extensive policies in place—including mandatory federal standards that apply to the bulk power system and nuclear power plants—to assure reliability. In addition, a number of mechanisms have been introduced to facilitate relevant information sharing between the public and private sectors, and within the power sector itself. But given the complexity, fast-changing nature, and magnitude of potential cyber threats, it is also clear that more must be done to improve grid cybersecurity. Urgent priorities include strengthening existing protections, for the distribution system as well as the bulk power system; enhancing coordination at all levels; and accelerating the development of robust protocols for response and recovery in the event of a successful attack.

This report summary highlights key findings and recommendations from the co-chairs of the Bipartisan Policy Center's (BPC) Electric Grid Cybersecurity Initiative. It covers four topic areas: standards and best practices, information sharing, response to a cyber attack, and paying for cybersecurity. Recommendations in these areas target Congress, federal government agencies, state public utilities commissions (PUCs), and industry. The Initiative was launched as a collaboration of BPC's Energy and Homeland Security Projects in May 2013. Its goal was to develop policies—aimed at government agencies as well as private companies—for protecting the North American electric grid from cyber attacks. To guide the Initiative, BPC assembled a diverse and highly knowledgeable advisory group that included cybersecurity experts and managers, grid operators, and former energy and national security officials. BPC also held a public workshop on August 6, 2013, in Washington, D.C., to solicit additional perspectives and insights. Information on the Initiative and materials from the workshop can be accessed at http://bipartisanpolicy.org/events/2013/08/protecting-electric-grid-cyber-attacks-where-do-we-stand. A more detailed discussion of these issues and additional recommendations can be found in the main report.

Standards and Best Practices

The U.S. bulk power system is already subject to mandatory federal reliability standards that include some cybersecurity protections. Critical infrastructure protection (CIP) standards are developed by the North American Electric Reliability

Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). These standards cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans. While standards provide a useful baseline level of cybersecurity, they do not create incentives for the continual improvement and adaptation needed to respond effectively to rapidly evolving cyber threats. Distribution facilities generally operate outside of FERC jurisdiction. In some cases attacks at the distribution-system level could have consequences that extend to the broader grid. Our recommendations in this area aim to elevate cybersecurity at both the bulk power system and at the distribution system levels.

A particularly important recommendation concerns the establishment of a new industry-led body, comprising power sector participants across North America and modeled on the nuclear power industry's Institute of Nuclear Power Operations (INPO). Based on experience with INPO, we believe such an organization could substantially advance cybersecurity risk-management practices across the industry and, in doing so, serve as a valuable complement to existing NERC standards. In addition, we offer recommendations aimed at encouraging participation in this new institute, managing cyber risks that may originate in the supply chain, and training a cybersecurity workforce.

- NERC should continue to develop and enforce cybersecurity standards in a manner that is consistent with a risk-management approach and that provides affected entities with compliance flexibility. FERC and applicable authorities in Canada should be supportive of this approach in their review of NERC standards.
- The electric power industry should establish an organization, similar to INPO, that would develop cybersecurity performance criteria and best practices for the entire industry. This new institute should include the full range of participants in the North American power sector, and it should engage in several activities, including (a) developing performance criteria and conducting detailed cybersecurity evaluations at individual facilities; (b) analyzing systemic risks, particularly on the distribution system; (c) analyzing cyber events as they occur and disseminating information about these events; (d) providing technical assistance, including assistance in the use of new cybersecurity tools; and (e) cybersecurity workforce training and accreditation.
- Congress should adopt legislation that would encourage power sector entities to participate in the new institute by providing liability protection to entities that achieve a favorable cybersecurity evaluation by that body.
- The federal government should provide backstop cybersecurity insurance until the private market develops more fully. Legislation modeled on the Terrorism Risk Insurance Act (TRIA) could extend reinsurance coverage to insurers following cybersecurity events that require payouts in excess of some predetermined amount. Such a backstop should be withdrawn gradually after the private insurance market has had sufficient time to develop.
- The electric power sector and the federal government should collaborate to establish a certification program that independently tests grid technologies and products to verify that a specified security standard has been met. Such a program would provide equipment manufacturers and vendors with a strong incentive to invest in cybersecurity features, and it would benefit utilities by allowing them to select products that incorporate such features.
- The National Institute of Standards and Technology (NIST) should include guidelines for related skills training and workforce development in its Cybersecurity Framework.

- DHS should work with universities and colleges to develop engineering and computer science curricula built around industrial control system cybersecurity. These curricula should include vulnerabilities and threat analysis. DHS should also coordinate with the Department of Defense to identify ways that some of the cybersecurity defense training undertaken by the military might be offered more broadly to personnel in critical infrastructure sectors.
- The U.S. Department of Energy (DOE) should assist states in providing funds so that regulatory staff can participate in academic programs, more intensive training institutes, and continuing education programs.

Information Sharing

Timely information sharing—between industry and government, within industry and across critical infrastructure sectors, and across government agencies and different levels of government—is an essential component of an effective cybersecurity strategy. It is also the primary way to identify, assess, and respond to threats in real time. While government and industry are doing a better job of sharing information on cyber threats, two fundamental challenges persist. The first is industry's reluctance to share data for fear of triggering regulatory non-compliance actions, violating privacy or antitrust protections, or potentially disclosing proprietary or confidential business information. A second challenge is obtaining intelligence information from government authorities that is sufficiently timely, specific, and actionable. Our recommendations target these issues as well as the need for enhanced information sharing with international and state-level counterparts, and across critical infrastructure sectors.

- Efforts to create a firewall between information sharing and regulatory compliance should continue, and additional steps should be taken to pursue the full functional separation of NERC (as a regulatory entity) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which is housed within NERC. For example, NERC could establish the ES-ISAC as a subsidiary of NERC, with ties only in funding, and physically separate the two organizations. Going forward, DOE and NERC should work with industry to evaluate whether and to what extent NERC's firewall policy improves industry's confidence that sharing timely information with NERC does not risk triggering potential compliance or enforcement action.
- Policymakers and federal agencies should work with industry to better understand how much sharing of customer data is needed to provide relevant threat and vulnerability information. This would help all parties gain a better understanding of how privacy concerns relate to electric grid cybersecurity.
- Congress and executive branch agencies should continue to develop information sharing provisions that balance concerns about customer privacy with the imperative for timely and effective information sharing.
- Congress should continue to pursue legislation that protects utilities from civil and criminal liability for "good faith" information sharing. The "good faith" standard should be defined in terms that are sufficiently clear and specific so as to minimize the risk of litigation; one component of this standard should require utilities to take all reasonable measures to remove personally identifiable information from shared data. In addition, Congress may wish to consider limiting liability protections to situations in which information is shared at the direction of, or with the permission of, government authorities.
- Efforts to streamline the security clearance process for selected power sector employees, as required by Executive Order 13636, should continue. At the same time, intelligence agencies should declassify relevant threat and vulnerability information when possible and use other methods, such as tear lines, to separate

classified and unclassified information in order to facilitate the sharing, for official use only, of otherwise classified or restricted reports with power sector partners.

- Utility-led efforts to collect and share information on threats and vulnerabilities should be expanded and should complement information sharing between the government and industry.
- DHS, the ES-ISAC, and industry should consider how to most efficiently share threat and intelligence information with trusted vendors.
- The U.S. intelligence community, DHS, and DOE should conduct regular outreach to state utility commissions, other relevant state agencies, and public and municipal utilities on cyber threats and vulnerabilities. These federal agencies should identify best practices for sharing classified information with private sector entities as needed to protect critical infrastructure.
- U.S. intelligence officials should conduct regular outreach and briefings, including classified briefings with relevant state officials and with Canadian and Mexican industry counterparts. DHS and DOE should also work to ensure that these counterparts are able to engage in all relevant government-industry forums.
- DHS should encourage organizational standardization to promote a more efficient flow of information between the Information Sharing and Analysis Centers (ISACs) of various critical infrastructure sectors and the government. In addition, mechanisms should be developed to facilitate direct industry-to-industry information sharing (or company-to-company) communication.

Responding to a Cyber Attack

A large-scale cyber attack on the electric grid would present governance and coordination challenges in addition to difficult technical and logistical challenges. Not only would a successful attack require cyber-specific responses, such as the removal of malware, it would likely also require more traditional disaster response operations to deal with resulting threats to public health and safety. Efficient and ongoing communication will clearly be critical, along with effective coordination, a clear chain-of-command, and the ability to adapt quickly as new information emerges. While Executive Order 13636 has helped clarify cybersecurity roles and responsibilities within the federal government, questions remain concerning the specific responsibilities of different agencies and chain-of-command in the event of an attack. We provide recommendations for improving government and industry readiness for a cyber event, and for reconciling differences between the existing National Response Framework (NRF) and the 2010 Interim National Cyber Incident Response Plan (NCIRP). The NRF, which was developed in 2008 and updated in 2010, was designed to address physical and other impacts from "traditional" disasters (such as a hurricanes or floods); by contrast, the NCIRP is specifically intended to respond to a cyber event.

- Federal policymakers should strengthen the governance and coordination framework for cyber-event response by (a) clarifying and further developing federal government chain-of-command and decision-making mechanisms; (b) clarifying the roles and responsibilities of different agencies; (c) strengthening protocols for government and industry interaction; (d) clarifying thresholds for federal involvement and conditions under which the Stafford Act would apply; (e) further developing the National Cyber Risk Alert Level (NCRAL) system; (f) updating information sharing protocols; and (g) better defining the roles, responsibilities, and authorities of the Unified Coordination Group, which is the interagency body with substantial responsibility for executing the NCRIP.
- The NCIRP should be changed to elevate the role of governors in the event of a successful cyber attack. More generally, improved integration is needed between the

NRF and NCIRP with respect to chains-of-command across government, coordinating mechanisms, thresholds for initiating response efforts and providing federal assistance, and state versus federal authority.

- Governors should further strengthen state-wide governance structures for cyber preparedness.
- Response protocols should provide clarity on the respective roles and responsibilities of law enforcement, who are seeking to preserve information for criminal investigations and public- and private-sector responders seeking to reestablish critical services.
- State and federal agencies and critical infrastructure operators should continue to conduct scenario exercises, such as the National Level Exercise, to practice responses to a cyber attack.

Paying for Electric Grid Cybersecurity

U.S. utilities are expected to spend about $7 billion on cybersecurity by 2020. An important question is how the costs of these investments will be distributed among utility shareholders and customers. Some entities will be able to seek cost recovery through FERC- or state-approved tariffs; for others, the ability to recover cybersecurity costs will depend on contract terms and market conditions. The challenge for regulators lies in determining whether a particular investment is prudent, or whether other needed investments are being overlooked. Unfortunately, many regulators lack the expertise to make these judgments. In addition, the task is complicated by the "public goods" nature of many cybersecurity investments. To the extent that the benefits of a given investment (or conversely, the costs of a failing to make the investment) extend beyond an individual company, that company can be expected to underinvest from the perspective of the system as a whole. Moreover, current regulatory processes tend to overlook systemic risks.

- DOE should fund efforts—to be undertaken via the new industry-led institute described previously—to understand systemic cyber risks, including risks involving interdependencies and the spillover of consequences from one firm or jurisdiction to another. DOE should also fund research to help regulators better evaluate the potential impacts of cyber attacks and weigh the benefits of cybersecurity investments.
- State PUCs should work with the new institute to normalize cybersecurity best practices and to increase confidence in cybersecurity-related cost-recovery decisions.
- DOE should work with industry and state regulators to develop metrics for evaluating utility investments in cybersecurity. Alternative approaches are conceivable, including approaches that focus on compliance with NERC CIP standards and/or guidance provided by the new industry-led institute. These metrics could then be used in cost-recovery determinations.
- Given the adaptive nature of cyber threats, regulation should encourage continuously improving cyber capabilities. This may require alternative regulatory models that go beyond a reasonable/unreasonable (pass/fail) test and that provide dynamic incentives for ongoing improvement.
- Policymakers and industry should consider supporting cybersecurity investments by entities that may own critical assets but that might otherwise fail to undertake these investments because of insufficient resources or an inability to recover costs. An assistance fund for these situations could be administered by the new institute.
- DOE should continue to advance cybersecurity research and development. Congress should continue to provide resources to enable this support.
- State and federal regulators should proactively engage with companies to establish priorities and needs that

companies have for improving their cybersecurity posture. Where possible, this can be undertaken outside of a docketed proceeding to minimize the risk of broadly disclosing vulnerabilities.

Conclusions and Next Steps

As noted throughout this report, the electric power industry and the government agencies that oversee it have already done much to improve grid cybersecurity. Our recommendations target areas where gaps or limitations in current policies and practices leave room to further reduce the vulnerability of the electric grid—and the broader U.S. economy—to fast-growing and rapidly evolving cyber threats. Several themes emerge across these recommendations, including the need for greater clarity about the roles and responsibilities of different entities, the need for effective public-private partnerships and improved information sharing, and the need to address incentives and cost-allocation issues in light of the diversity of parties involved and the "public good" nature of many cybersecurity investments.

In the coming months, BPC staff and Initiative co-chairs will reach out to policymakers and stakeholders to advance the recommendations outlined in this report. At the same time, BPC will work to advance progress on challenges that would remain even if all these recommendations were adopted, such as addressing the privacy concerns that continue to present a stumbling block for legislative efforts to enhance information sharing between industry and government. Going forward, BPC's Homeland Security Project will explore further options to resolve these challenges. In the coming months, BPC's Energy Project plans to address the broader issue of electric grid resilience, including the role of modern grid technologies and practices in addressing multiple threats (e.g., weather, physical, cyber, geomagnetic) to the grid.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 1: Introduction

Cyber threats to North America's electric grid are growing, making electric grid cybersecurity an increasingly important national and international issue. The Federal Bureau of Investigation (FBI) recently noted that cyber attacks are eclipsing terrorism as the primary threat facing the United States.[1] As cyber attacks become more frequent, energy systems are increasingly being targeted. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is part of the U.S. Department of Homeland Security (DHS), reported responding to 198 cyber incidents in fiscal year 2012 across all critical infrastructure sectors. Forty-one percent of these incidents involved the energy sector, particularly electricity.[2]

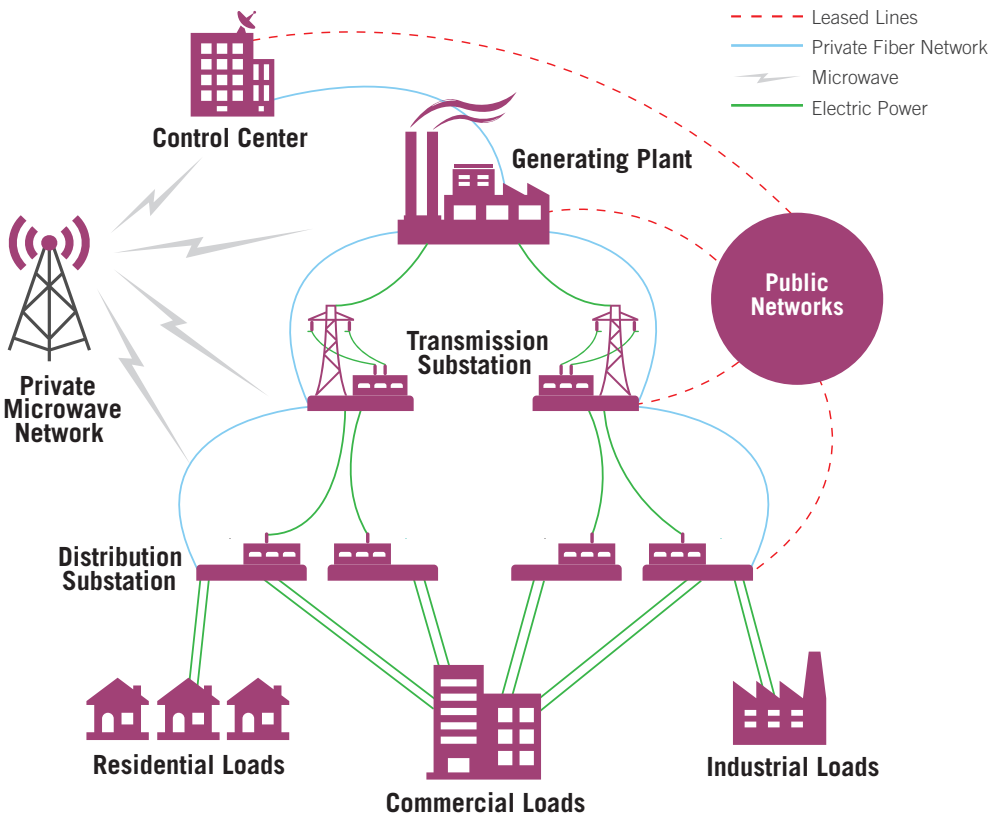
Fortunately, the electric power sector has yet to experience a cyber attack that affected the operations of the North American grid. But experts generally agree that the risk of a large-scale attack is significant and must be addressed.[3] The costs and impacts of such an event could be profound. The 2003 Northeast blackout showed that any extended grid failure could have a large price tag. That multiday blackout, which was attributed to a tree branch in Ohio, not a cyber attack, affected an estimated 50 million people in the United States and Canada and was estimated to cost about $6 billion.[4] A large-scale cyber attack or combined cyber and physical attack could potentially lead to even larger costs, triggering sustained power outages over large portions of the electric grid and prolonged disruptions in communications, food and water supplies, and health care delivery.[5]

Unlike traditional threats to electric grid reliability, such as extreme weather events, a cyber attack is less predictable in its timing and potentially more difficult to diagnose and address. A cyber attack could also be combined with a more traditional physical attack to distract authorities and inflict further damage. A cyber attack could come from many sources and target many potential vulnerabilities. The North American electric grid is sprawling and complex, with approximately 476,000 miles of high-voltage transmission lines,[6] and thousands of power plants, distribution lines, and substations. Figure 1 depicts the various components of the electric grid. The ongoing incorporation of "smart grid" technologies adds an additional layer of complexity to the system. While the addition of these technologies can generate a number of new efficiencies and other benefits, from a cybersecurity perspective, the transition from analog to digital controls creates new potential pathways into utility systems and thus new security challenges for utilities, system operators, and regulators.

The cyber threats facing the electric grid are numerous and constantly evolving. Threats can come from a variety of malicious actors, such as foreign nations, terrorist organizations, private firms, external hackers, or internal "bad actors" among system operators, power companies, and vendors. These actors may seek to disrupt grid operations, damage infrastructure, or steal information. Poor cybersecurity hygiene or simple negligence on the part of system operators, utility personnel, and vendors, as well as from unanticipated interactions between systems (e.g., following software or hardware installation) or device failure pose another set of risks.

To secure the grid against damage from threats that seek to exploit its cyber vulnerabilities, these vulnerabilities must be understood and defensive measures must then be taken to reduce both the opportunity for exploits and the consequences of unintended action. As the U.S. Government Accountability Office (GAO) has noted, "The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt critical services, including electric power."[7] Potential vulnerabilities are numerous and include an increasing number of entry points to the system, the integration of new system and network technologies, an increase in connectivity across the system, and the expanding volume

Figure 1. Overview of the Electric Power System and Control Communications



Source: U.S. Department of Energy (2011) Roadmap to Achieve Energy Delivery Systems Cybersecurity, Energy Sector Control Systems Working Group. September, p. 62. Available at: http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

of customer information being collected by utilities.[8] The growing prevalence of information and communications technology on the grid and the large number of industry personnel with access to this technology create an evolving cybersecurity environment where the relative importance of specific vulnerabilities may change as new types of attacks become possible.[9]

Managing cybersecurity risks on the electric grid raises challenges unlike those in more traditional business IT networks and systems. Energy control systems are uniquely designed and operated to control real-time physical processes that deliver continuous and reliable power. As such, they require security solutions that meet unique performance requirements and operational

needs. Cybersecurity technologies that are developed to protect business IT computer systems and networks can inadvertently damage an energy-delivery control system.

The policy and regulatory structure that currently governs electric grid cybersecurity is complex. This complexity stems from the multifaceted energy, commerce, and national security interests that are at stake, as well as from the governance structure of—and multitude of entities within—the electricity sector itself. Numerous federal, state, and local agencies—along with relevant government bodies in Canada and Mexico—are involved in some aspect of grid cybersecurity, whether their activities include setting standards, collecting intelligence on threats, sharing information, making cost-recovery determinations, or responding to cyber attacks.

In many ways, the electric power sector is in a stronger position to address cyber threats than other sectors, as it already has mandatory standards—enforced at the federal level in the United States—that apply to the bulk power system.[10] The bulk power system is generally composed of high-voltage transmission facilities and large generation facilities, but does not include small electric generators or the distribution systems that are used to distribute power to local customers. The reliability of such local distribution facilities and small generators is governed by state government regulators (provincial in Canada), or in the case of municipalities and rural electric cooperatives, local government boards and commissions. Mandatory federal cybersecurity standards therefore apply only to the bulk power system facilities and do not extend to the electric distribution system. Given this complex regulatory structure, achieving an adequate level of cybersecurity across the electric grid as a whole is a challenge for industry and policymakers.

Successfully managing cyber risks and recovering from a destructive cyber attack requires effective coordination at several levels, including coordination between U.S. energy companies, the intelligence community, and emergency management agencies; between relevant federal government and state and local authorities; and between U.S. energy regulatory and security agencies and their counterparts in Canada and Mexico. Coordination between power sector entities and government agencies at all levels is also essential. While a number of mechanisms are already in place for sharing information across jurisdictions, between the public and private sectors, and within the power sector itself, we believe these mechanisms could be improved. While government and industry have made progress in developing and practicing protocols for response[11] and restoration following a large-scale cyber attack, it will be necessary to resolve differences that remain between the frameworks that govern cyber attack response and traditional disaster response, so as to establish the chain-of-command among federal agencies and clearly define the roles and responsibilities of different government agencies and the electric power industry itself.

One key policy challenge is that current economic and institutional factors may be keeping power sector investments in cybersecurity—including investments in research and development—below socially optimal levels. First, given the interconnected nature of the grid, the benefits of these investments are likely to extend beyond the footprint of an individual company. Because the company making the investment is unlikely to be able to capture these spillover benefits, many companies may limit their investments to a level that is suboptimal from the perspective of the grid as a whole. Second, since the risks and consequences of a cyber attack are difficult to estimate and quantify, individual companies may have a difficult time determining which investments to make beyond the minimum required for compliance with mandatory standards. Further, current compliance and enforcement programs for bulk power system cybersecurity standards

Box 1. Examples of Cyber Attacks on Energy Systems

Stuxnet. The Stuxnet computer worm was discovered in 2010 and gained attention for the damage it caused at a nuclear facility in Iran. It was designed to attack nuclear centrifuge rotors in two ways, by aiming to over-pressurize centrifuges and by trying to over-speed the rotors. The attack has been studied as the first real-world deployment of a cyber-physical attack, highlighting the power of malware to disrupt operations and damage equipment.

Aurora. The U.S. government staged the Aurora event in March 2007 at the U.S. DOE's Idaho facility. The planned cyber attack on a generator control system led to the destruction of the generator and a fire.

Slammer. The Microsoft SQL Server worm, Slammer, infected a private computer network at the idled Davis-Besse nuclear power plant in Ohio in January 2003. The worm disabled a safety-monitoring system for several hours and led to a temporary failure of the plant's process computer.

Night Dragon. McAfee, the security technology company, named a series of cyber attacks focused on global oil, gas, and petrochemical companies "Night Dragon." The Night Dragon attacks started in November 2009 and led to the theft of proprietary and confidential information.

Phishing attacks. Phishing attacks at an electric bulk provider and an electric utility in 2011 led DHS to deploy incident response teams. The teams identified malware and found evidence of a sophisticated threat actor.

Shamoon. The national oil company of Saudi Arabia, Aramco, reported in 2012 that the computer virus Shamoon was responsible for damaging about 30,000 computers in an effort to disrupt gas and oil production. The attack did not stop production, because system software for technical operations was not impaired. However, it was one the most destructive cyber attacks against a single company.

Sources:

California Public Utilities Commission (2012) Cybersecurity and the Evolving Role of State Regulation, pp. 5-6. Available at: http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf.

U.S. Government Accountability Office (2012) Cybersecurity: Challenges in Securing the Electricity Grid, pp. 11-12. Available at: http://www.gao.gov/assets/600/592508.pdf.

Ralph Langner (2013) To Kill a Centrifuge: A Technical Analysis of What Stutnex's Creators tried to Achieve. Available at: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

McAfee (2011) Global Energy Cyberattacks: "Night Dragon." Available at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

Reuters (2012) "Aramco Says Cyberattack Was Aimed at Production," The New York Times, December 9. Available at: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

fail to reward—instead they potentially penalize—entities that go beyond minimal compliance. For utility regulators, evaluating cybersecurity investments is a challenge, as they must balance the benefits of potential improvements to grid security against the costs that are allowed to be passed through to ratepayers. Finally, investing in cybersecurity may be particularly difficult for smaller entities with limited resources, including municipal utilities and rural electric cooperatives. This is problematic because these smaller entities may nonetheless be interconnected to the larger system.

Against this background of an evolving threat, a complex and overlapping governance structure, and barriers to sufficient investment, we believe that traditional, standards-based methods for protecting the grid must be augmented by innovative new approaches. One is the establishment of an industry-wide organization—modeled on the Institute for Nuclear Power Operations (INPO)—to advance cybersecurity practices across the industry. We expect that such an organization—coupled with appropriate incentives for participation such as insurance policies and liability protection—could do much to improve cybersecurity across the industry. Other approaches that we recommend rely on public-private partnerships that would mobilize the respective assets and expertise of industry and government agencies, and improve the flow of information between government and industry and across different companies.

This report provides findings and recommendations from the co-chairs of the Bipartisan Policy Center's (BPC) Electric Grid Cybersecurity Initiative. Launched in May 2013 as a collaborative effort of BPC's Energy and Homeland Security Projects, the Initiative sought to develop policies—aimed at government agencies as well as private companies—to protect the North American electric grid from cyber attacks. The recommendations in this report were crafted with the help of an advisory group that included power sector cybersecurity experts and managers, grid operators, and former energy and national security officials. The report is organized as follows: Chapter 2 provides an overview of the current landscape for electric grid cybersecurity governance. Chapter 3 focuses on policy issues and recommendations for standards and best practices. Chapter 4 makes recommendations with respect to information sharing between industry and government, and across government agencies and industries. Chapter 5 makes recommendations for organizing response operations in the event of a successful cyber attack. Chapter 6 discusses recommendations for funding cybersecurity investments, including recommendations concerning the assignment of cybersecurity costs. Chapter 7 summarizes conclusions and identifies next steps.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 2: The Existing Landscape for Electric Grid Cybersecurity Governance

In the United States, the federal government and states share a role protecting the electric system against cyber attacks. Several federal agencies have responsibilities pertaining to electric grid cybersecurity, including the Federal Energy Regulatory Commission (FERC), U.S. Department of Energy (DOE), DHS, and the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce (DOC). State public utility commissions (PUCs) regulate electricity distribution systems and many generation facilities operated by investor-owned utilities—and, in some cases, rural cooperatives and municipal utilities—and therefore also play an important role in electric grid cybersecurity. Generally speaking, however, municipal utilities and rural electric cooperatives operate with oversight by local governments or utility boards.

In Canada—a key partner for the United States in the effort to enhance the cybersecurity of the electric grid—there is a different division of governmental responsibilities, with the federal public safety department mandated to mitigate cyber threats to all critical infrastructure sectors and with provincial governments responsible for oversight of electric reliability standards.

This section provides a summary of current federal government efforts to improve grid cybersecurity, highlighting President Obama's recent executive order and the ongoing activities of relevant federal agencies. It also provides a summary of recent legislative proposals and highlights efforts at the state level and in Canada, as well as recent industry initiatives.

Executive Order 13636

In February 2013, the White House issued an executive order titled "Improving Critical Infrastructure Cybersecurity" and an accompanying Presidential Policy Directive. Executive Order 13636 aims to improve the sharing of information regarding cyber threats between government and private actors, including classified information.[12] The executive order also requires DHS to identify critical infrastructure that could be vulnerable to cyber attack with potentially catastrophic regional or national consequences, and to assess the privacy and civil liberty risks associated with its programs.[13] Finally, the executive order directs the NIST to develop a Cybersecurity Framework that addresses cyber risks and is applicable to multiple sectors and industries.[14] In February 2014, NIST released Version 1.0 of its Cybersecurity Framework.[15] The framework attempts to build on existing standards and practices in critical infrastructure industries to enable companies to: "1) describe their current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders."[16] While the framework is voluntary, it could eventually form the basis for future state or federal regulations or otherwise set the "standard of care" for purposes of assessing liability in the wake of a cyber event.[17]

Box 2. Overview of NIST Cybersecurity Framework

A 2013 executive order from President Obama directed NIST to create a cybersecurity framework. The preliminary Cybersecurity Framework was released in October 2013. Version 1.0 was released in February 2014.

- The Cybersecurity Framework is intended to be used by owners and operators of critical infrastructure across the 16 critical infrastructure sectors to provide guidance on how to manage cybersecurity risks.
- The framework is voluntary and is built on existing standards, guidance, and best practices.
- It is intended to supplement, not replace, an organization's existing cybersecurity plan. However, the Cybersecurity Framework can be used to help organizations draft a cybersecurity plan if they do not have one.
- The framework is divided into three components:

1. *The Framework Core* maps out cybersecurity activities that are common across all critical infrastructures, including the electricity sector. The core is intended to help organizations describe security standards and best practices. It is also intended to help organizations talk about these standards and practices, despite varying levels of technical expertise within the organization.
2. *The Framework Profile* provides organizations with a tool to map out their current cybersecurity state as well as a desired state with improved security. The tool allows organizations to consider relevant legal or regulatory requirements, best practices, and organization and sector goals.
3. *The Framework Implementation Tiers* allow organizations to describe their cybersecurity practices by assigning them to one of four descriptive tiers. These tiers range from Partial (Tier 1) to Adaptive (Tier 4), with higher tiers representing greater sophistication of risk-management practices and integration of these practices into the organization's larger risk-management practices. The tier selection process weighs numerous factors, including the organization's risk-management practice, the threat environment, and legal or regulatory requirements.

Federal Energy Regulatory Commission and North American Electric Reliability Corporation

FERC is responsible for ensuring the reliability of the bulk power system. Under authority granted by the Energy Policy Act of 2005, FERC designated the North American Electric Reliability Corporation (NERC) as the Electricity Reliability Organization responsible for developing mandatory and enforceable reliability standards in the United States. (As discussed further below, NERC has also been formally recognized by applicable government authorities in Canada.) These reliability standards address issues relevant to the operation of existing, new, and modified bulk-power facilities, including critical infrastructure protection (CIP).[18] CIP standards cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security,

incident reporting and response planning, and recovery plans. CIP version 5, the most recent set of standards, was approved in 2013.[19]

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

NERC also issues email alerts to disseminate actionable information necessary to ensure the reliability of the bulk power system.[20] NERC alerts are categorized into three levels: industry advisories, which are purely informational and do not require a response; recommendations to industry, which recommend specific actions by registered entities and require a response as indicated; and essential actions, which identify specific actions necessary for reliability and require a response as defined in the alert.

NERC's role in information sharing extends to its operation of the ES-ISAC. The ES-ISAC establishes situational awareness, incident management, and coordination and communication capabilities with the electricity sector through timely, reliable, and secure information exchange. The ES-ISAC shares critical information with electric industry participants regarding infrastructure protection.[21] The goal is to promptly disseminate threat indications, analyses, and warnings and issue alerts to assist electricity sector participants in taking protective action. In addition to its information sharing and coordination roles, the ES-ISAC's other responsibilities include analyzing event data, working with the ISACs for other critical infrastructure sectors to exchange information and assistance, performing cyber risk assessments, and participating in critical infrastructure exercises and industry outreach.[22]

NERC participates in a number of other activities aimed at improving electric grid cybersecurity. For example, NERC's Grid Security Exercise (GridEx)[23] allows companies to validate their response to simulated physical and cyber incidents. More than 200 organizations from the United States, Canada, and Mexico participated in the 2013 GridEx, making it the largest sector-specific security exercise. NERC's annual Grid Security Conference (GridSecCon)[24] provides an opportunity to discuss emerging cyber threats and best practices and provides training opportunities. NERC also participates in a number of cybersecurity initiatives led by DHS, DOE, and Canadian government organizations.

Department of Energy

DOE does not have a regulatory role related to electric grid cybersecurity. Instead, the agency supports private industry though technological development and coordination. DOE has been designated as the lead agency for the energy sector in the National Infrastructure Protection Plan. DOE's roles in this capacity include providing situational awareness to stakeholders in coordination with DHS and other government agencies; collaborating with DHS and Energy Government Coordinating Council (GCC) partners to clarify the roles of sector partners and facilitate cooperation with energy stakeholders; and work with DHS and Energy GCC partners to improve coordination of resilience activities.[25]

DOE initiatives include the Cybersecurity for Energy Delivery Systems (CEDS) program, which sponsors research and development to improve cyber defenses,[26] as well as a number of other efforts to help prepare electrical

system owners and operators for a potential cyber attack. DOE recently announced $30 million in awards for the development of tools and technologies to strengthen cybersecurity on the electric grid and oil and gas system infrastructure.[27] CEDS program activities fall under five project areas, guided by the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*:[28]

- "*Build a Culture of Security.* Through extensive training, education, and communication, cybersecurity 'best practices' are encouraged to be reflexive and expected among all stakeholders.
- *Assess and Monitor Risk*. Develop tools to assist stakeholders in assessing their security posture to enable them to accelerate their ability to mitigate potential risks.
- *Develop and Implement New Protective Measures to Reduce Risk*. Through rigorous research, development, and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems.
- *Manage Incidents*. Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery, and restoration capabilities.
- *Sustain Security Improvements*. Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring."[29]

In addition, DOE works with DHS and sector stakeholders to coordinate the development of the Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2), which was designed to support the development and measurement of cybersecurity capabilities within the power sector.[30] The model allows companies to evaluate, prioritize, and improve cybersecurity activities by allowing them to make comparisons between their activities and industry-vetted practices.[31] DOE also collaborated with NIST and NERC to develop the electricity Risk Management Process (RMP) guideline.[32] The RMP is intended to enable participants in the electric power sector to apply effective cybersecurity risk-management processes that can be tailored to an individual organization's needs. DOE is also working on an inter-organizational initiative to improve cyber threat information sharing between DHS, DOE, law enforcement, and the intelligence community, with the goal of establishing a common framework for sharing cyber threat indicators at near real-time speed.

Department of Homeland Security

DHS is the designated lead federal agency responsible for the cybersecurity of critical infrastructure in the United States. The agency plays an important role in coordinating the dissemination of information to private entities that own and operate the nation's electrical systems and in responding to sophisticated cyber attacks. In the former role, DHS manages numerous information sharing partnerships to help public and private entities keep one another informed on cyber trends and threats. For example, DHS's National Cybersecurity and Communications Integration Center (NCCIC) works with federal agencies; state, local, and international governments; and industry to share information and enhance situational awareness, preparedness, and response.[33] DHS also houses the ICS-CERT, which responds to and analyzes cyber incidents on industrial control systems, and also disseminates information on threats and vulnerabilities.[34] Additionally, national domestic cyber attack response teams and infrastructure improvement research projects are housed under DHS. Finally, DHS has conducted a series of cyber event response exercises—known as Cyber Storm—with the private sector and with federal, state, and international government partners.[35]

National Institute of Standards and Technology

Under the 2007 Energy Independence and Security Act, Congress directed NIST to coordinate the development of a voluntary framework for smart grid protocols and standards, including cybersecurity protocols. The aim was to enable and improve interoperability between systems. In 2010, NIST's Smart Grid Interoperability Panel finalized its *Guidelines for Smart Grid Cyber Security*.[36] In addition, under Executive Order 13636 (February 2013), NIST is responsible for coordinating a voluntary framework for standards, methodologies, procedures, and processes to help owners and operators of critical infrastructure identify, assess, and manage cyber risks in a cost-effective, flexible manner. As noted above, NIST released Version 1.0 of its Cybersecurity Framework in February of 2014.[37]

Recent Legislative Proposals

A handful of bills that address electric sector cybersecurity have been introduced in Congress in recent years. So far, none of these bills has been signed into law. However, recent legislative proposals have helped to shape the debate about what the federal government can and should do to manage cyber risks facing critical infrastructure.

The Cyber Intelligence Sharing and Protection Act of 2013 (CISPA)[38] was passed by the U.S. House of Representatives in 2013; it has yet to be taken up for consideration by the U.S. Senate. If signed into law, CISPA would clear the way for increased information sharing between the federal government; state, local, and tribal governments; and private companies. For example, the bill calls on the Office of the Director of National Intelligence to establish procedures for sharing classified cyber intelligence with private sector entities that have the appropriate security clearances. The stated goal is to help "protect, prevent, mitigate, respond to, and recover from cyber incidents."[39]

In the Senate, debate continues on the extent to which new information sharing legislation such as CISPA should require additional privacy protections for personal data.

The Cybersecurity Enhancement Act of 2013 passed the U.S. House of Representatives in 2013. The bill contains provisions to guide federal assessment of cyber risk; guide federal cybersecurity research and development; enable NIST to develop standards and processes to harden federal networks; and establish a federal-university-private sector task force to coordinate research and development and improve workforce training.[40] A similar bill, the Cybersecurity Act of 2013 was introduced in the U.S. Senate in July 2013 but has not been passed. The bill calls for an "ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness." Specific provisions call for federal support of voluntary, industry-led standards to help reduce cyber risks and for the creation of a federal cybersecurity research and development plan.[41]

The Electric Grid Cybersecurity Act of 2012 was introduced in the Senate in the 112th Congress. It would have given the federal government broad authority to address cybersecurity concerns. It called for the creation of a National Cybersecurity Council, which would have worked with the private sector to conduct risk assessments to determine which critical infrastructure assets are most vulnerable to cyber threats. Another provision would have consolidated the nation's cybersecurity efforts under the auspices of a new National Center for Cybersecurity and Communications.[42]

State Activities

The federal government does not have oversight authority over the reliability of local distribution facilities. Investor-owned electric distribution companies, which serve the majority of U.S. households, are regulated by state PUCs,[43] which are responsible for the safety and reliability of the portions of the grid within their state and for ensuring that the electricity rates paid by utility customers are reasonable. State PUCs have traditionally required facilities in their jurisdiction to implement reliability measures on the distribution network, including the adequacy and security of such facilities, and have begun to engage in oversight of utility cybersecurity. Through ratemaking decisions, state PUCs determine which investments and expenses utilities may pass on to customers.[44]

Through their regulatory capacities, state PUCs play an important role in determining what cybersecurity measures utilities should be required to implement on the distribution system, as well as how the costs of these investments should be divided between ratepayers and shareholders, and how associated expenditures should be audited. Additionally, state PUCs (and sometimes state legislatures) develop policies to govern the sharing of information between utilities, regulators, third-party vendors, and the public.

State regulators have begun taking significant steps to address cyber risks to the electric grid. The National Association of Regulatory Utility Commissioners (NARUC) has undertaken a number of efforts to elevate cybersecurity at state utility commissions. In February 2010, NARUC passed its "Resolution Regarding Cybersecurity." The resolution called on commissioners to be vigilant against potential cyber threats, prepared to prevent an attack, and ready to mitigate the harmful consequences of an attack. It encouraged commissioners to regularly review their own policies and procedures to ensure consistency with applicable standards and best practices and to work with regulated utilities to ensure that they are prepared for a cyber attack and in compliance with existing standards.[45] In August 2013, NARUC passed an additional resolution—"Resolution Regarding Cybersecurity Awareness and Initiatives"—that called on commissioners to continue to give a high priority to monitoring cybersecurity threats; to become increasingly knowledgeable about cybersecurity threats to relevant utility sectors; to maintain an open dialogue with their regulated utilities to ensure that adequate resources are being applied to deter, detect, and respond to cyber attacks; and to continue to partner with federal, regional, and state agencies and industry organizations to enhance cybersecurity.[46] NARUC has also issued guidance concerning cybersecurity measures to state regulators that includes questions state PUCs should pose to their regulated utilities.[47] It also conducts trainings and outreach to state PUCs on cybersecurity issues, as well as regular briefings on the threat landscape.

In most states, commissions have not been required by state statutes to establish cybersecurity standards or to provide incentives for effective cyber governance. However, state regulators are enhancing their oversight of electric utility cybersecurity practices in a variety of ways. Although not a comprehensive list, it is worth noting several illustrative examples of recent state commission activities:

- Under the Pennsylvania Utility Code, utilities are required to maintain physical security, cybersecurity, emergency response, and business continuity plans; self-certify compliance with this requirement; and report cyber and/or physical attacks that cause more than $50,000 in damages or interrupt service to customers.[48] Pennsylvania's cybersecurity requirements extend beyond the bulk power system to the customer meter. For larger utilities, Pennsylvania Commission staff reviews these plans as part of a management audit at least once every five years.

- In Texas, the PUC's rules on advanced metering infrastructure (AMI) require compliance with cybersecurity standards specified by an independent meter data-management organization, the regional transmission organization, or the PUC, as well as independent security audits of investor-owned utilities that are deploying AMI.[49] The Texas PUC has continued the practice of conducting annual security audits. PUC staff has also participated and encouraged utilities and other stakeholders to participate in voluntary standards development activities, including activities of the Institute of Electrical and Electronics Engineers, the International Society of Automation, and the North American Energy Standards Board.[50]
- In Ohio, the PUC initiated a cybersecurity audit of the largest smart grid deployment in the state to assess the extent to which the implementing utility, Duke Energy Ohio, was incorporating NIST guidelines and industry best practices, and to identify areas for improvement. The Ohio PUC has sponsored cybersecurity workshops with the state's utilities and with its state and federal agency partners (including DHS, DOE, and the FBI). It has also initiated training sessions for industry stakeholders and solicited comments on how to best address cybersecurity issues. Finally, Ohio PUC staff has participated in standards development efforts.[51]
- The Missouri Public Service Commission requires all Missouri utilities under its jurisdiction to have reliability plans in place; it also requires electric utilities to certify compliance with FERC Order 706 concerning the adoption of NERC CIP standards.[52]
- The New York Public Service Commission's Office of Utility Security monitors utility security planning, implementation, and performance; evaluates the effectiveness of both physical and cybersecurity systems; analyzes security-related incidents; monitors technical developments related to infrastructure security; coordinates on broader critical infrastructure protection issues with the New York State Office of Homeland Security; and evaluates emerging technologies for continually improving security.[53] Generally, the commission uses existing NERC CIP standards as benchmarks for the adequacy of utility cybersecurity measures.[54]
- Washington state is currently working to develop cybersecurity reporting requirements for utilities. These requirements cover standard practice, reporting cyber events, and information requirements for rate recovery. A discussion draft was released in November 2013.[55]

Beyond state PUCs, a number of other state agencies and offices have a role to play in protecting the electric grid from cyber threats. These include governors' offices, state energy offices, state CIOs, and, in the event of a successful attack, state homeland security, emergency management, and law enforcement agencies. In recognition of the important role of governors, the National Governors Association has created a new Resource Center for State Cybersecurity. The resource center will consider the need for state policy to ensure adequate cybersecurity for state-owned and state-based infrastructure.[56]

Cybersecurity Governance in Canada

As noted above, the governance model in Canada with respect to cybersecurity differs in several distinct ways from that which is in place in the United States. Most importantly, there is one federal department tasked with coordinating efforts to secure vital cybersecurity systems, while oversight and enforcement of NERC CIP standards is conducted by provincial authorities.

Public Safety Canada

Established in 2003, PSC's mandate is to coordinate the activities of all federal departments and agencies in Canada

responsible for national security and public safety.[57] In many respects, its mandate mirrors that of DHS, including in its oversight of independent agencies tasked with core national security and public safety functions: the Canada Border Services Agency, which manages Canada's borders; the Canadian Security Intelligence Service, which serves as the primary national intelligence body; and the Royal Canadian Mounted Police, which is the national police service. PSC also oversees the Canadian Cyber Incident Response Centre (CCIRC), which is the Canadian equivalent of DHS's U.S. Computer Emergency Readiness Team (US-CERT).

Like DHS, PSC is the designated lead federal agency in Canada on cybersecurity. It is mandated with coordinating implementation of Canada's Cyber Security Strategy.[58] Released in 2010, the strategy identifies three pillars for protecting digital infrastructure in the country: (1) securing government systems, (2) partnering to secure vital cyber systems outside the federal government, and (3) helping Canadians to be secure online.

Also like DHS, PSC performs a critical role in coordinating the dissemination of information to critical infrastructure owners and operators and the response to cybersecurity incidents. Signature initiatives in this regard include formalized partnerships to engage critical infrastructure sectors and government agencies at all levels through the National Cross-Sector Forum[59] as well as the development of a cross-sectoral agreement for improved information sharing.

Both prior and subsequent to establishment of the strategy, PSC has enjoyed a close working partnership with DHS, including around cooperation on common cybersecurity challenges. In fact, under the February 2011 declaration *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness* by President Obama and Canadian Prime Minister Stephen Harper, PSC and DHS are lead agencies on enhancing the resiliency of critical infrastructure and cybersecurity—one of the four key priorities identified in the agreement.[60] And, in step with the Beyond the Border objectives, in late 2012, PSC and DHS announced a Cybersecurity Action Plan to strengthen cybersecurity cooperation.[61]

Unlike the respective missions of DHS and PSC, there are no direct Canadian equivalents to FERC or DOE.[62]

Provincial Oversight of NERC Reliability Standards

As noted above, the responsibility for ensuring bulk power system reliability in Canada rests with provincial governments, not with any federal agency. In 2002, Ontario became the first jurisdiction in North America to make NERC's electric reliability standards mandatory and enforceable.[63] Since then, each of the provinces that comprise the Canadian portion of the integrated North American grid has employed one or a combination of several governance mechanisms to formally recognize NERC's role for developing mandatory and enforceable standards (e.g., a memorandum of understanding [MOU], legislation, regulation, or market rules). Provincial authorities in Canada are therefore key players as well in the context of government efforts aimed at enhancing cybersecurity protection of the North American grid.

Ongoing Electric Sector Activities

Individual power companies as well as power sector trade associations have undertaken a range of activities to advance electric grid cybersecurity. One key activity is participation in the recently re-launched Electricity Sub-sector Coordinating Council (ESCC). The ESCC provides a mechanism by which CEO-level utility personnel can engage with each other and relevant government agencies in an effort to "foster and facilitate the coordination of sector-wide policy-related activities and initiatives to improve the reliability and resilience of the Electricity Sub-sector."[64]

Throughout the industry, companies and organizations are coordinating with federal and state agencies as they implement the activities described above. For example, many investor-owned utilities, public utilities, and electric cooperatives collaborated with DOE and DHS to develop and pilot the ES-C2M2. In addition, a number of power sector companies, in conjunction with the ES-ISAC, DOE, Pacific Northwest National Laboratory, and Argonne National Laboratory, are participating in the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a pilot program that provides a near-real-time capability for critical infrastructure owners and operators to share and analyze cyber threat data and receive machine-to-machine mitigation measures.[65]

Industry trade associations, in addition to coordinating with each other and with the federal government, have undertaken a number of activities for their own members. The American Public Power Association has conducted member outreach, published cybersecurity guidance,[66] and offered training on cybersecurity issues. The National Rural Electric Cooperative Association published a guidance document for its members that includes best practices for improving cybersecurity and mitigating the cyber risks associated with the deployment of new technologies, such as smart grid technologies.[67] The Edison Electric Institute has developed the Threat Scenario Project, which identifies threat scenarios and practices for threat mitigation.[68] And, north of the border, the Canadian Electricity Association has entered into a formal MOU with PSC's CCIRC for sharing cybersecurity information.[69] This MOU is expected to serve as a template for other such agreements with critical infrastructure sectors.

Box 3. An Example of an Innovative Utility and Government Partnership for Cybersecurity

Snohomish County Public Utility District (SnoPUD) and the Air Force National Guard (AFNG) are currently discussing a joint cybersecurity collaborative exercise. The scope of work being discussed would include the AFNG performing penetration and vulnerability testing for SnoPUD over a two- to four-week period. During this time, the AFNG would gain experience with the utility industry and learn about controls systems and utility cyber architecture. SnoPUD would be able to observe how hackers might approach attacking their system, and learn how to better monitor their system during an attack.

Under the scope of work being discussed, the team plans to use SnoPUD's Smart Grid lab, which is designed to precisely simulate the utility's production environment. The lab includes the systems and field equipment for EMS/SCADA, Distribution Management, Distribution Automation, Field Area Network and Substation Automation. Use of SnoPud's Smart Grid lab will provide tremendous insight to the AFNG on utilities' Smart Grid architecture and systems. It will also provide SnoPUD insights into how the utility can better secure its Smart Grid.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 3: Standards and Best Practices for Cybersecurity

Our recommendations concerning standards and best practices for cybersecurity address multiple policy objectives. These include creating standards and best practices that enable effective risk management; encouraging formation of, and broad industry participation in, a new industry-led organization focused on advancing cybersecurity; improving supply chain security; and training a cybersecurity workforce.

Create Standards and Best Practices that Enable Effective Risk Management

Cybersecurity standards, whether mandatory, such as those developed by NERC for the bulk power system, or voluntary, such as those adopted by many distribution system utilities, provide a baseline level of cybersecurity (or "floor"). However, standards alone are insufficient for managing cybersecurity risks. Additional mechanisms are needed to encourage greater investment in cybersecurity risk management and governance, while also reaching beyond the bulk power system to the distribution system to address sources of systemic risk. Tools made available by DOE—namely the ES-C2M2 and the RMP guidelines—help to fill this gap. We believe the establishment of a new organization—which would complement the existing CIP standards process at NERC—for the electric industry to address grid cybersecurity could provide an effective vehicle for advancing cybersecurity excellence across the entire industry.

Bulk Power System: Key Challenges

Currently, only the bulk power system is subject to mandatory standards for cybersecurity. The Energy Policy Act of 2005 charged FERC with certifying an Electricity Reliability Organization to develop reliability standards for the bulk power system, including standards addressing cybersecurity.[70] Under this authority, FERC certified NERC to develop and enforce mandatory reliability standards, with FERC oversight.[71] (As discussed in Chapter 2, NERC has also been formally recognized by applicable government authorities in Canada.) These mandatory standards are designed to provide for reliable operation of the bulk power system. NERC's reliability standards cover a range of activities[72] and include CIP measures, which encompass cybersecurity. NERC's first set of CIP standards was approved by FERC in 2008.[73] The CIP standards address eight areas of electricity sector operations:

- Critical cyber asset identification;
- Security management controls;
- Personnel and training;
- Electronic security;
- Physical security of critical cyber assets;
- Systems security;
- Incident reporting and response planning; and
- Recovery plans for critical cyber assets.[74]

NERC's standards are important to the overall cybersecurity strategy for the power sector—they establish a baseline level of protection against cyber attacks for the highly interconnected bulk power system and have been integral to the industry's progress toward addressing cybersecurity risks. However, while some might argue for a broader expansion of mandatory standards to advance cybersecurity across the grid,[75] policymakers should resist emphasizing reliance on standards at the expense of better developing complementary approaches. The rapidly evolving nature of cyber threats means that the standards development process is unlikely to move fast enough to keep pace with the latest threat information. In addition, as discussed below, standards can lead to a focus on compliance at the expense of an overarching cybersecurity strategy.

The existing process for implementing and enforcing NERC's CIP standards helps companies achieve a minimum level of cybersecurity, but may discourage them from taking more aggressive actions or implementing system-wide protections. NERC and FERC's current enforcement model, which subjects most potential violations to an enforcement process, has discouraged companies from adopting more stringent internal compliance programs. For example, under the current approach, entities that adopt a more stringent system of internal controls—in other words, that go above and beyond the minimum required by current standards—may face increased exposure to civil penalties as a result of identifying more instances of potential noncompliance with the standards.[76]

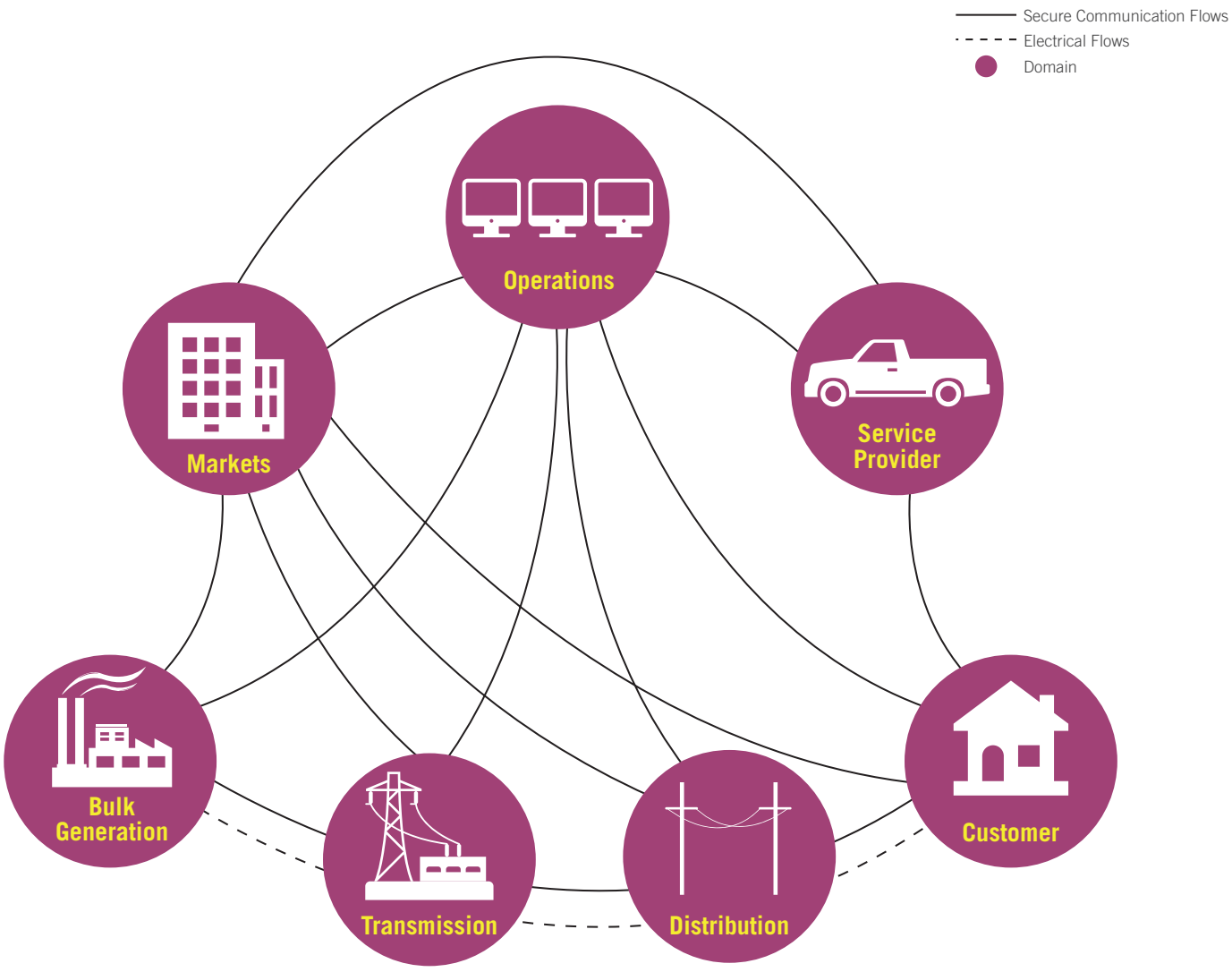
The most recent (version 5) CIP standards included certain language that allowed a greater focus on internal controls. In November 2013, FERC approved the CIP standards, but directed NERC to modify this to clarify compliance requirements. However, FERC did express support for an enforcement approach that is risk-based.[77] Movement toward a risk-based enforcement approach should help to alleviate the compliance risk that utilities currently face in developing more robust cybersecurity programs than the minimum baseline requirements needed for compliance.

Distribution System: Key Challenges

Beyond the bulk power system, distribution system operators in the United States operate outside FERC jurisdiction and thus do not face mandatory cybersecurity standards. Nationwide, roughly 3,200 distribution utilities are responsible for delivering electricity to retail customers. While most of these utilities (roughly 2,000) are publicly owned, investor-owned utilities account for the majority (about 63 percent) of retail electricity sales.[78] As noted in the previous section, investor-owned utilities are typically operated under the jurisdiction of state PUCS. Rural cooperatives and municipal utilities are typically governed by boards of directors or local governments.

From the perspective of federal policymakers, a key question is the degree to which cybersecurity events on distribution systems could have implications for the bulk power system, or for broader national security or economic interests. In some cases, cyber attacks on distribution system facilities could have consequences that extend beyond that system. For example, simultaneous attacks on multiple distribution utilities, or an attack on a single utility's distribution operations in multiple locations, could have broader ramifications for the bulk power system. In addition, electric distribution systems carry power to pipelines, water systems, telecommunications, and other critical infrastructure, while also serving critical government or military facilities. Distribution-level cyber attacks that disrupt electric service to such facilities could have important economic and security consequences. Finally, as the grid continues to modernize over the next few decades, the lines between transmission and distribution systems may become increasingly blurred, creating challenges for the management of cybersecurity risks and the traditional jurisdictional divide. (See Figure 2.) For example, many analysts are projecting an increased role for distributed generation systems that are engineered to accommodate two-way power flows. This evolution could increase the likelihood that cyber events at the distribution level would pose a risk to the bulk power system, and it points to a growing need for coordination across the entire electric power sector.

Figure 2. Electrical and Communication Flows among Participants on the Modernized Grid



Source: NIST (2010) Smart Grid Framework 1.0, January. Available at: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Two recent legislative proposals have attempted to extend cybersecurity standards beyond the bulk power system to assets that are deemed vital to the national interest—though neither of these has become law. The Grid Reliability and Infrastructure Defense (GRID) Act, which passed the U.S. House of Representatives in 2010, would have given FERC the authority to set cybersecurity standards for "defense critical electric infrastructure" outside the bulk power system.[79] The Grid Cybersecurity Act of 2011, which passed out of the U.S. Senate Energy and Natural Resources Committee, likewise would have allowed FERC to set cybersecurity standards for "critical electric infrastructure."[80]

In the absence of mandatory cybersecurity standards at the distribution level, voluntary standards have provided some guidance on cybersecurity measures for distribution systems. NIST has incorporated NERC's CIP standards in its Smart Grid Interoperability Framework. Though not mandatory, these standards have been adopted (and thus applied to distribution systems) by some utilities, though as GAO has noted, federal and state regulators have not coordinated to monitor the actual implementation of voluntarily adopted standards.[81] As noted in Chapter 2, under Executive Order 13636, NIST has developed a Cybersecurity Framework, which is likely to function as a set of voluntary cybersecurity standards for the electric power sector.

Cooperation within the industry and industry-government partnerships have also helped utilities make progress toward addressing cybersecurity risks to the distribution system (as well as the bulk power system). For example, DOE, in collaboration with DHS and industry, developed the ES-C2M2 to help utilities and grid operators assess their cybersecurity capabilities and prioritize investments in improving cybersecurity.[82] In addition, many companies across the power sector have collaborated to exchange information on best practices through organizations such as the North American Transmission Forum and the U.S. National Electric Sector Cybersecurity Organization[83] which is jointly funded by DOE and by participating utilities. In addition, as noted in the previous section, the ESCC enables utility executives in both the United States and Canada to regularly engage with government officials to facilitate and support activities aimed at improving the reliability and resilience of the power sector.

A second key question for federal policymakers is whether the addition of mandatory cybersecurity standards for distribution systems would provide a cost-effective means of managing the risk that a cyber attack on the distribution system could threaten the electric grid or national economic or security interests. Given the longstanding line of jurisdiction that has separated the bulk power system from local distribution systems, our view is that there would have to be a very compelling policy argument to consider changing the current jurisdictional balance in favor of granting additional authority to FERC. At present, we do not believe that there is a sufficient case for expanding FERC's jurisdiction to encompass cybersecurity at the level of the distribution system, or that such a solution would be the most effective means of elevating cybersecurity protections across the grid. As noted above, the NERC CIP standards do play an important role in establishing a baseline level of cybersecurity on the bulk power system, but they also tend to promote a narrow focus on compliance and are unlikely to evolve rapidly enough to keep pace with changing cyber threats. In addition, states and utilities tend to have better knowledge of conditions on distribution systems than federal regulators; indeed, because these systems are diverse and present differing vulnerabilities for the larger system, a more individualized approach is likely justified.

While the electric power sector has made important progress toward improving grid cybersecurity over the last few years, a new mechanism is needed to complement existing standards in a way that allows individual

utilities—and the sector as a whole—to foster a culture of cybersecurity excellence. As discussed below, we believe that a new organization is the best mechanism to do that.

Complementing Existing Standards and Policies With a New Organization

We believe that a new, industry-wide organization, composed of power sector participants across North America, could advance cybersecurity risk-management practices across the industry and, in doing so, serve as a valuable complement to the existing NERC standards framework. Such an organization could be modeled after the nuclear power industry's INPO, which was formed largely in response to the 1979 accident at Three Mile Island. At the time, a commission appointed by President Carter to investigate the accident reached the conclusion that "merely meeting the requirements of a government regulation does not guarantee safety. Therefore, the industry must also set and police its own standards of excellence to ensure the effective management and safe operation of nuclear power plants."[84] INPO is widely viewed as an effective organization that has succeeded in improving the safety and performance of nuclear power plant operations in the United States and abroad.[85] It performs four primary activities:

- *Evaluations.* INPO establishes performance objectives, criteria, and guidelines for the commercial nuclear industry and performs nuclear plant and corporate evaluations. More than 1,600 evaluations have been performed. Nuclear plants are subjected to comprehensive, on-site evaluations approximately every two years.[86] Based on their performances, plants are given numerical grades. Results are then presented confidentially to the utility CEO in the presence of line management.[87] Plant operators respond to these assessment reports by identifying actions to address problems flagged during the evaluation.
- *Training and Accreditation.* INPO's National Academy for Nuclear Training provides training and support for nuclear power professionals at its national training facility in Atlanta. Additionally, selected operator and technical training programs are accredited through INPO's National Nuclear Accrediting Board.
- *Event Analysis.* INPO assists in reviewing significant events at nuclear facilities. It communicates best practices and lessons learned through information exchanges and publications.
- *Assistance.* At the request of a nuclear plant operator, INPO will provide assistance with technical or management issues related to plant operations or support.

INPO is a nonprofit corporation that does not engage in advocacy. It has a staff of 400 nuclear power professionals and an annual budget of nearly $100 million,[88] funded by member dues. The INPO board of directors includes CEOs and senior executives from nuclear utilities and plant operators. INPO's governance structure also provides for an advisory committee that has included independent nuclear experts and retired regulators.

A number of factors are often cited as playing an important role in INPO's success. These include regular CEO engagement, a specific focus on safety, broad industry support, a mechanism for ensuring that member entities are held accountable, and independence from individual utilities and the Nuclear Regulatory Commission. In addition, INPO has procedures in place to prevent conflicts of interest.[89] Buy-in from the insurance industry has also been important. All nuclear power plants carry coverage through the industry's collective insurance provider, Nuclear Electric Insurance, Ltd. (NEIL). NEIL requires INPO membership as a condition of insurability and uses INPO ratings as a factor in setting insurance premiums. We believe that an organization with an analogous mandate

and operating conditions to INPO could provide an effective mechanism for promoting cybersecurity excellence within the power sector.

Recommendations

- NERC should continue to develop and enforce cybersecurity standards in a manner that is consistent with a risk-management approach and that provides affected entities with compliance flexibility. FERC and applicable authorities in Canada should be supportive of this approach in their review of NERC standards.
- The electric power industry should establish an organization, similar to INPO, that would develop cybersecurity performance criteria and best practices for the entire industry. This organization would be intended to complement the standards process that is in place at NERC. We encourage the industry to establish such an organization before a significant cybersecurity event occurs and requires a rapid response. A centralized, industry-governed institution may be in the best position to promote effective strategies for managing cyber threats that could have broader systemic impacts. This effort should include the full range of generation, transmission, and distribution providers and market operators in the North American power sector, including municipal utilities and electric cooperatives. It should be funded through member dues. We envision that this organization—which we will call, for purposes of this discussion, the Institute for Electric Grid Cybersecurity (hereafter, the institute)—would be charged with several activities:

  - *Development of performance criteria and cybersecurity evaluations*. The institute would develop performance criteria and best practices for cybersecurity and perform detailed evaluations of individual facilities according to these criteria. Performance criteria and best practices should be tailored to address conditions for individual companies and systems, taking into account their contribution to larger systemic risks.
  - *Analysis of systemic risks*. With industry's assistance, the institute should conduct analyses to identify facilities or locations on the system, and in particular the distribution system, where a localized cyber event could have disproportionate implications for the broader electric grid or for economic or national security. For example, there may be places on the grid where, because of system interdependencies, the loss of a particular substation could trigger a cascade of impacts in multiple critical infrastructure sectors. While many utilities have taken inventories to identify critical facilities or customers, a broader national inventory, combined with modeling and scenario analysis, should help to identify priority areas for cybersecurity investment from the perspective of protecting the grid as a whole.
  - *Event analysis*. While NERC, FERC, state and provincial agencies, and potentially federal law enforcement or intelligence agencies are likely to be involved in analyzing significant cybersecurity events, the institute should play a role in understanding the cause of such events and disseminating lessons learned.
  - *Technical assistance*. The institute should provide technical support to entities that need assistance implementing performance criteria. It should also facilitate the use of cybersecurity tools—such as the ES-C2M2—produced by industry and government partnerships.
  - *Training and accreditation*. The institute should engage in efforts to define positions and career paths for utility cybersecurity professionals. The institute could partner with, or potentially house, ongoing efforts to develop cybersecurity certifications.

A key challenge for any organization that seeks to represent the electric power industry as a whole, in contrast to the much smaller population of nuclear plant operators and utilities involved in INPO, involves effectively engaging the large number and diversity of players that are part of the industry. For the new organization to fully represent the sector, it would need to include public and investor-owned utilities, independent generation and transmission providers, and regional transmission operators across North America. This large number of entities could impede efforts to reach consensus on best practices, limit the institute's ability to encourage meaningful changes to performance, and potentially create challenges for information security. Careful consideration must therefore be given to structuring the organization and governance of the institute in ways that will help manage and alleviate the conflicts and resource inequities that could arise with such a diversity of participants.

Finally, we would encourage federal policymakers to consider participation in the institute—and satisfactory performance evaluations—as equivalent to adopting the Cybersecurity Framework to the extent adoption of the framework is required to be eligible for particular government programs or incentives going forward.

Encouraging Participation in the Institute for Electric Grid Cybersecurity

We believe most utilities would see clear benefits to participating in a new cybersecurity organization. Such an organization could reduce pressure on Congress or FERC to extend more aggressive or widespread regulatory measures, offer helpful technical assistance and information, and give participants the opportunity to develop new norms for cost-recovery practices. However, given the "public good" nature of cybersecurity investments, additional incentives are likely to be helpful to encourage participation in this new organization. For example, membership in the institute could be tied to liability protection and improved access to cybersecurity insurance against first-party economic losses.[90] Policy recommendations aimed at facilitating these incentives for participation are described below.

Liability Protections

In most cases, regulated utilities receive protection against liability for consequential damages arising from service disruptions through their tariffs, which generally cover liability for damages from outages that result from ordinary negligence (the precise degree of liability protection varies across jurisdictions).[91] In the context of cyber threats, power sector entities face two sources of liability exposure. The first is liability associated with sharing information with the federal government, other companies, or other non-governmental entities. These liability concerns are discussed in Chapter 4. The second is liability exposure from actions an entity either takes or does not take in response to information. For example, a utility could be sued if an action taken in response to information about a cyber threat—such as interrupting service—harms another entity. Conversely, a utility could also be subject to lawsuits if it decides to take no action in response to information and outages ensue.[92]

Existing legislative proposals have attempted to provide liability protections for entities that act upon certain types of information. For example, CISPA protects actions that are taken "in good faith" to respond to threat information received by the acting entity, though it is not clear what the phrase "in good faith" would mean in practice or if invoking CISPA could create conflicts with the protections afforded by a utility's existing tariff.

Legislation that grants clear liability protections to utilities that participate in the institute could provide a valuable incentive for participation. However, given the challenges

of passing such significant legislation in Congress, establishment of the institute should not be held back in the absence of legislation. Considering how federal liability protection would interact with state and other laws that govern utility liability will be a key challenge for policymakers.

Cybersecurity Insurance

Cybersecurity insurance would limit the potential economic losses at individual entities experiencing a cyber attack or event, and insurance underwriting practices could provide incentives for individual entities to implement strong cybersecurity measures. At present, cybersecurity insurance does exist; however, coverage for utility companies is limited and often expensive.[93]

The purpose of such insurance is to mitigate losses from cyber events such as data breaches, network damage, or cyber extortion.[94] The existing market for cybersecurity insurance covers some third-party cyber-related losses, such as losses impacting an entity's customers from breaches of its IT systems. However, only limited coverage is available to companies, such as electric utilities, that are looking to insure against direct losses from a cyber attack.[95]

Several factors stand in the way of widespread corporate cyber insurance coverage. First, insurance carriers need better data to underwrite such policies, including actuarial data about cyber-related losses and statistical data about the frequency of cybersecurity incidents. Developing these data presents a significant challenge for insurance providers, given the difficulty of quantifying the value of, and assigning liability to, cybersecurity-related losses; the fact that the costs of a cyber attack may extend to entities beyond the target of the attack; and the reluctance of many entities to share data on cybersecurity events.[96] Lacking better information, carriers that offer insurance against cyber attacks may price premiums so high as to make these policies unaffordable.[97] Second, insurers may face a lack of demand for such policies, because many companies falsely believe that they are already insured against the effects of a cyber attack. Finally, insurance carriers worry that a successful cyber attack in the near term could lead to a "cyber hurricane" of large claims before sufficient reserves are built up to cover the losses.[98]

Another question for power sector entities and other operators of critical infrastructure is how the insurance market can address large-scale events with both cyber and physical components (e.g., a cyber attack that leads to infrastructure damage). Developing appropriate insurance mechanisms for these situations would require a better understanding of how cyber events might unfold on the grid and improved information sharing about risks among relevant stakeholders.[99]

The Obama administration is considering how insurance might play a role in implementing the Cybersecurity Framework. For example, a recent White House blog post discussed working with the insurance industry to "build underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing and foster a competitive cyber insurance market."[100]

A more robust insurance market for cyber risks would help to foster the adoption of cybersecurity best practices while reducing the potential costs of a cyber event for individual companies. We applaud the administration's efforts to include insurance companies in discussions surrounding the development of NIST's Cybersecurity Framework. Policy efforts to build a more robust insurance market will increase utilities' incentive to participate in the institute as a way to demonstrate effective cyber risk management to insurers. In turn, the standards and practices set by the institute, as well as the results from individual utility evaluations, will provide important information to insurers in developing and pricing their products.

Recommendations

- Legislation modeled on the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act could encourage utilities to participate in the institute and comply with the practices that it establishes. The SAFETY Act provides liability protection for qualified anti-terrorism products or services, provided a requisite level of insurance coverage has been purchased. While the SAFETY Act targets developers of anti-terrorism products, legislation designed to promote electric sector cybersecurity could provide similar liability protection to entities that achieve a favorable evaluation by the institute.
- The federal government should provide backstop cybersecurity insurance until the private market develops more fully. Legislation modeled on the Terrorism Risk Insurance Act (TRIA) could create a U.S. government reinsurance facility to extend reinsurance coverage to insurers following cybersecurity events that require payouts in excess of some predetermined amount. A federal backstop would increase carriers' willingness to offer cyber insurance and lower the cost of doing so. In addition, a federal backstop would give carriers time to gather and review data about cyber incidents as they seek to develop policies that appropriately share risk.[101] Such a backstop should be withdrawn gradually after the private market has had sufficient time to develop.[102]
- DHS, DOE, and the ES-ISAC should work closely with the insurance industry to improve tools and methods for quantifying cybersecurity risks and valuing cybersecurity protections.

Improve Supply Chain Security

Managing cybersecurity risks that originate in the supply chain is another important challenge facing the electric industry. Vulnerabilities arise when utilities procure hardware and software from third-party vendors, including hardware or software that is intended to support smart grid and cybersecurity initiatives. New products and software may not be sufficiently secure in their design or implementation; they may be subject to malicious manipulation or be compromised by the use of counterfeit parts. Suppliers may not face market pressures or requirements to incorporate cybersecurity features in the design of their systems and devices. In some cases, products sold to the power sector may be insecure by design or insufficiently supported as new risks are identified. These issues are further complicated by the global nature of supply chains, which offer multiple possible entry points for cyber attacks. For example, numerous SCADA (supervisory control and data acquisition) devices are manufactured overseas, including in China, where external cyber threats have originated in the past.[103]

A number of efforts are underway to address challenges in this area. The National SCADA Test Bed, created in 2003, utilizes the research expertise and capabilities of DOE's National Laboratories to conduct testing, research, technology development, and training to address cyber risks, including supply chain vulnerabilities. For example, the Pacific Northwest National Laboratory is working with partners to develop an integrated suite of open-source tools and techniques to identify vulnerabilities in the hardware, firmware, and software components of energy delivery systems. This effort encompasses tools that can be used locally to provide hardware supply chain assurances as well as larger-scale computing services for analyzing systems to identify potential concerns in critical infrastructure supply chains.[104]

Box 4. The SAFETY Act and TRIA

In the wake of the September 11, 2001, terrorist attacks, Congress signed into law the SAFETY Act and TRIA.

SAFETY Act. Passed in 2002, the SAFETY Act is part of the Homeland Security Act of 2002. The act provides liability protection for the sellers of qualified anti-terrorism products, services, or software in the event of a terrorist attack. This protection is intended to support the development and commercialization of anti-terrorism devices by mitigating the manufacturers' and sellers' liability fears. As of May 2013, DHS had approved 600 products, services, and software technologies for liability protection under the SAFETY Act.

The Safety Act allows for two levels of liability protection: Designation and Certification.

Designation. This category is reserved for products, services, or software that meet a range of specifications, such as demonstrating proven utility and effectiveness as well being able to be immediately deployed. The SAFETY Act offers sellers of "designated technologies" liability limited to the amount of liability insurance that DHS determines they must maintain. The act provides for the same liability protections for the sellers of promising products, services, or software that are undergoing developmental testing and evaluation.

Certification. Products, services, or software that meet the requirements for "designation" can achieve "certification" status by meeting several additional benchmarks, such as performing as intended and being safe for use as intended. In addition to the liability protections offered to "designated technologies," the sellers of products, services, and software that achieve "certification" can assert the Government Contractor Defense in the case of a terrorism-related claim.

TRIA. TRIA was also signed into law in 2002 and has been extended several times. Under current law, TRIA is set to expire at the end of 2014. TRIA is intended to ensure that terrorism insurance covering commercial property and casualty is both available and affordable. It was set up to provide public and private compensation for qualified privately-insured losses, with the government administering a reinsurance program in the form of a federal backstop.

Act of Terrorism. TRIA only covers acts of terrorism that are certified by the federal government. Since 2007, this has included both domestic and foreign acts of terrorism.

Mandatory Coverage. The act requires private insurers to offer terrorism insurance as part of their commercial property and casualty insurance policies. However, individual policyholders are not mandated to purchase the terrorism insurance. In addition, TRIA does not mandate specific prices for the policies.

Recommendations

- The electric power sector and the federal government should collaborate to establish a certification program that independently tests grid technologies and software to verify that a specified cybersecurity standard has been met. This program could potentially build upon the testing and certification programs being developed under the Smart Grid Interoperability Panel, or potentially be conducted with an independent testing and certification organization such as Underwriters Laboratories.[105] Such a program would provide equipment manufacturers and vendors with a strong incentive to invest in cybersecurity features, and it would benefit power sector entities by allowing them to select products that incorporate tested cybersecurity features.

Train a Cybersecurity Workforce

Enhancing electric sector cybersecurity will require a workforce that is trained to manage cyber vulnerabilities and adapt to evolving cyber threats to industrial control and automation systems. Workers with specialized skills will be needed to build cybersecurity features into the electric grid and to maintain and improve cybersecurity for the foreseeable future. Currently, the industry's workforce does not have sufficient expertise in these areas.

In developing its Cybersecurity Framework, NIST has emphasized cybersecurity workforce as an area that needs improvement and further collaboration with relevant sectors and standards-development organizations.[106] NIST has noted that "[w]hile it is widely known that there is a shortage of general cybersecurity experts, there is also a shortage of qualified cybersecurity experts with an understanding of the specific challenges posed to critical infrastructure."[107]A recent collaborative effort between critical infrastructure asset owners, vendors, training organizations, and standards bodies, has led to the development of a new certification program—the Global Industrial Cyber Security Professional (GICSP) Certification[108]—which is intended to ensure baseline set of knowledge, skills, and abilities for professionals responsible for industrial control system cybersecurity.[109] Programs such as this could be an important tool for promoting a strong cybersecurity workforce in the electric power sector and other critical infrastructure sectors and could potentially be conducted in partnership with the institute discussed above.

Improving cybersecurity will also require well-trained federal and state regulators. Regulatory agencies need trained personnel to review utility governance, expenditures, and performance in this area. Currently, at the state level, larger commissions might have a small number of staff members who have had significant involvement with cybersecurity issues. At smaller commissions, there may be only a handful of staff members addressing the full suite of electricity-sector issues. While NARUC, DOE, and existing regulatory training institutes have made progress in providing general introductory training on these issues, more in-depth knowledge is needed to enable regulatory staff to effectively evaluate utility cybersecurity plans and responses to cyber events.

Proposed legislation has included measures aimed at building a stronger cybersecurity workforce. The Cybersecurity Act of 2013,[110] introduced in July and reported by the U.S. Senate Committee on Commerce, Science, and Transportation, includes a number of such measures. It directs DOC, the National Science Foundation (NSF), and DHS to support competitions and challenges to recruit cybersecurity talent or to stimulate cybersecurity innovations. It also directs NSF to continue an existing cybersecurity scholarship for service program. Finally, it requires NSF and DHS to arrange for the National Academy of Sciences to conduct a study of existing education, accreditation, training, and certification programs for professional development in information infrastructure and cybersecurity.

Recommendations

- We applaud NIST's recognition of the importance of developing a strong cybersecurity workforce for the nation's critical infrastructure sectors. We encourage NIST to include guidelines for related skills training and workforce development, including an understanding of industrial control system technologies, in future versions of its Cybersecurity Framework.
- DHS should work with engineering and computer-science programs at identified universities and colleges to develop specific curricula built around industrial control system cybersecurity. These curricula should include vulnerabilities and threat analysis. DHS should also coordinate with the Department of Defense to identify ways the cybersecurity defense training undertaken by the military might be offered more broadly to personnel in critical infrastructure sectors.
- Utilities should engage with cybersecurity training programs at universities or at state and local levels to ensure that such programs incorporate relevant training.
- DOE should assist states in providing funds so that regulatory staff can participate in academic programs, more intensive training institutes, and continuing education programs. Such programs will help regulatory agencies better understand strengths and gaps in security programs when approving investments, provide a bridge across the critical infrastructure sectors regulated by state commissions, and build relationships across jurisdictions that may be exposed to similar cyber risks. Scholarships for cybersecurity training may have to flow through NARUC or a comparable organization to ensure that state commissions can accept these funds.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 4: Information Sharing

Sharing actionable information on threats and vulnerabilities in a timely manner is one cornerstone of an effective cybersecurity strategy for the electric grid. This information sharing must occur along several dimensions—bilaterally between industry and government, within industry and across critical infrastructure sectors, and across government agencies and different levels of government. Even with an extensive array of mandatory or voluntary standards, cyber threats will inevitably evolve faster than new standards. Close collaboration and information sharing between the government and private sector is the primary way to identify, assess, and respond to threats in real time. While information sharing between government and industry has improved, two fundamental challenges persist. The first is industry's reluctance to share data with government and other private sector entities due to concerns over the potential for regulatory compliance actions, potential privacy or antitrust liability, and possible public disclosure of information. To share information on potential security risks with government authorities, utilities must feel confident that these concerns have been addressed. A second barrier to information sharing is the difficulty of obtaining intelligence information from government authorities that is sufficiently timely, specific, and actionable. The recommendations discussed in this section target several issues pertaining to information sharing, including legal risks to utilities, security clearances for utility and other electric industry personnel and access to intelligence data, information sharing by the federal government with international and state counterparts, and information sharing across critical infrastructure sectors.

Address Legal Risks and Information Disclosure Concerns

Potential Compliance Risks

As discussed in Chapter 2, the ES-ISAC is the primary portal through which utilities and other electricity industry participants currently share threat information with, or receive threat information from, the federal government. From an organizational standpoint, locating the ES-ISAC within NERC has created challenges for industry with respect to information sharing. Because NERC is a compliance organization with the authority and mandate to impose significant monetary penalties for compliance violations, entities that are subject to NERC reliability standards may be reluctant to share certain types of information with the ES-ISAC for fear of triggering a NERC audit or investigation.[111] In recognition of this issue, NERC's Board of Trustees acted in March 2013 to formally implement a firewall between the ES-ISAC and NERC's Compliance Monitoring and Enforcement Program.

NERC's policy states:

> To underscore the importance of a free flow of information to the ES-ISAC and to promote the kind of information sharing that is critical to maintaining the security of the electric system, NERC management believes it is important to affirmatively state that the ES-ISAC and ES-ISAC personnel have no responsibilities for the NERC Compliance Monitoring and Enforcement Program. Therefore, ES-ISAC personnel shall not, directly or indirectly, report or convey information about possible violations they may encounter or learn about in the course of their ES-ISAC activities to the compliance monitoring and enforcement program or to personnel assigned to that program. Similarly, compliance monitoring and enforcement personnel shall not, directly or indirectly,

obtain or seek to obtain information about possible violations of Reliability Standards from ES-ISAC personnel.[112]

In addition, DOE issued a letter in March of 2013 supporting the ES-ISAC's efforts at NERC and the revised policy statement that clarifies the "firewall between the ES-ISAC and the NERC Compliance Monitoring and Enforcement Program," noting that NERC's policy statement signals to the sector that the ES-ISAC will not share information with enforcement staff.[113]

Given that the formal establishment of a firewall is recent, it is not yet clear if this change will provide industry with sufficient confidence to share all relevant cyber threat or vulnerability information.

Privacy Laws

A utility that shares customer information, whether with a government agency or an industry information clearinghouse, risks being accused of violating privacy laws. Privacy advocates and utility customers are particularly concerned about the sharing of data that contain personally identifiable information from customers and about the possibility that this information could be disclosed or used inappropriately to investigate ordinary individuals or their activities.[114]

Privacy obligations for electric utilities are typically governed by state law or regulation,[115] or by internal utility policies. State laws and regulations can be enforced in state courts and by utility regulatory commissions. Utilities that depart from privacy policies can be held liable through an "unfair and deceptive trade practices" action at the Federal Trade Commission or an analogous state procedure.[116] As technologies such as advanced metering continue to change the volume and granularity of data being collected by utilities, utilities' exposure to liability for violating privacy protections may increase. Laws such as the federal Electronic Communications Privacy Act of 1986 (ECPA),[117] which was intended to address the use of customer data by telecommunications companies, and similar state laws, may eventually apply to data that utilities share with the federal government in response to a potential cyber threat.[118] Information sharing that is deemed to be in violation of ECPA could expose utilities to criminal penalties as well as private civil liability.[119]

Stakeholders and policymakers should be aware that the vast majority of time, individual customer data are not relevant to the threat information that utilities or other power sector entities would share with the government. In that sense, the power sector is distinct from the telecommunications industry, where personally identifiable information may be a critical piece of any threat information shared with government. For example, threats associated with industrial control systems would be observed and relayed to government without involving information on individual customers. However, the emergence of new power sector technologies, such as advanced metering, has added to the perception that customer privacy may be at stake. Effectively addressing these privacy concerns will be important for the success of any legislative proposal.

Antitrust Laws

In the context of sharing information with other power sector entities, trade associations, or other organizations, entities are concerned about the potential for liability or scrutiny under antitrust law. The most relevant law is the Sherman Antitrust Act ("Sherman Act"),[120] which broadly forbids collaboration that is undertaken in such a way as to restrain trade.[121] In addition to federal civil and criminal enforcement by the U.S. Department of Justice (DOJ), the Sherman Act may be enforced by a private plaintiff. In addition, most states have adopted antitrust laws, which often mirror the federal antitrust regime.

Information sharing for cybersecurity purposes does not seem to have, to date, prompted antitrust litigation. This is likely because industry collaborations that do not result in higher prices or reduced output are generally reviewed by DOJ under the "rule of reason" standard, which seeks to weigh the potential competitive benefits of the collaboration against potential competitive harms.[122] In 2000, DOJ was asked to review a data-sharing platform proposed by the Electric Power Research Institute (EPRI) to enable electric-industry participants to share information for cybersecurity purposes. Through its "business review letter" procedure, which DOJ uses to undertake such ex ante reviews, DOJ emphasized those features of an information sharing program that would be important from the standpoint of addressing antitrust concerns:

> Your request asserts that EPRI has adopted a number of measurers to lessen the possibility that its proposed information exchange will have any anticompetitive effects. The information to be exchanged will be strictly limited in nature; all information exchanged will relate directly to physical and cyber-security. There will not be any discussion of specific prices for equipment, electronic information or communications systems. No company-specific competitively sensitive information, i.e., prices, capacity or future plans, will be exchanged through the EIS program.[123]

DOJ further stated that it was not inclined to pursue antitrust enforcement action against EPRI, but reserved the right to do so in the future should anti-competitive effects be identified.[124] While the reasoning in this DOJ analysis provides a helpful window into how the DOJ will likely view cybersecurity-related information sharing among competitors, it has no protective effect for current or future information sharing efforts, whether undertaken by EPRI or others in the industry.[125] Prior information sharing proposals have contained express antitrust law exemptions,[126] which likely reinforces the perception that a legal "safe harbor" is needed before power sector competitors can confidently participate in cybersecurity information sharing. However, good faith industry information sharing to address electric grid cybersecurity threats is unlikely to raise a legal liability under the rule of reason.

Protection of Proprietary or Confidential Business Information

Power sector entities may hesitate to share data with government authorities or other entities in order to protect proprietary or confidential business information. Sharing information that is protected under a non-disclosure agreement, in particular, could expose utilities to lawsuits for breach of contract.[127] In addition, entities may fear that information shared with government agencies could be released through the Freedom of Information Act, similar open government laws at the state level, or—should the information be deemed to constitute ex parte communications—as a result of existing agency rules or judicial doctrine governing such communications.[128]

Information Sharing Liability Protections for Utilities Under CISPA and Executive Order 13636

Several recent legislative proposals, most notably CISPA,[129] have contained language that exempts certain information sharing from liability. CISPA provides protection from civil and criminal liability at the federal and state levels for entities acting in good faith to obtain or share information about cyber threats. However, it is not clear how the "in good faith" standard would be interpreted by courts or if this exemption is sufficiently specific to reduce the threat of litigation.[130]

While Executive Order 13636 does not directly address the liability risks utilities might incur by sharing information, it directs DHS, the DOC, and the U.S. Department of the Treasury to identify incentives for participation in the voluntary framework. (Though it is not clear what sorts of information sharing activities might eventually be embodied in the framework.)[131]

Recommendations

- We applaud NERC's efforts to create a firewall between information sharing at the ES-ISAC and compliance, which should help to assuage industry concerns about sharing information. To further address these concerns, additional steps should be taken to pursue the full functional separation of NERC (as a regulatory entity) and the ES-ISAC. For example, NERC could establish the ES-ISAC as a subsidiary of NERC, with ties only in funding, and physically separate the two organizations. Going forward, DOE and NERC should work with industry to evaluate whether and to what extent such changes improve industry's confidence that sharing timely information with NERC does not risk triggering potential compliance or enforcement action.
- Congress and executive branch agencies should work with industry to better understand the extent to which—for a grid that increasingly incorporates "smart" technologies—threat and vulnerability information shared with the federal government would actually require the sharing of customer data. This would help all parties understand to what extent privacy concerns are directly relevant to efforts aimed at improving the cybersecurity of the electric grid.
- Congress and executive branch agencies should continue to develop information sharing provisions that balance concerns about customer privacy with the imperative for timely and effective information sharing.
- Congress should continue to pursue cybersecurity legislation that protects power sector entities from civil and criminal liability, as well as information disclosure, for "good faith" information sharing. To meet the "good faith" standard, individual entities should be required to take all reasonable measures to ensure that personally identifiable information is removed from customer data. "Good faith" should also be defined in terms that are specific enough to minimize the risk of litigation. Finally, Congress may wish to consider further limiting liability protections to situations in which information is shared at the direction of, or with the permission of, government authorities.

Increase Security Clearances and Access to Intelligence Data

Much of the U.S. government's data and intelligence on cyber threats is subject to some level of classification and therefore can only be disseminated to individuals with the appropriate security clearances. This limitation, combined with government's tendency, according to some observers, to over-classify information,[132] makes it difficult for industry to effectively receive and utilize government intelligence information. State regulators and power sector employees (with the exception of those employed by federal utilities) are not federal government employees or contractors and must therefore go through a cumbersome process to obtain needed security clearances.[133] Executive Order 13636 addressed this issue, in part by directing the DHS secretary to streamline the security clearance process for non-federal employees of companies that are participating in the NIST Cybersecurity Framework. However, additional authority from Congress may be needed to ensure that private companies receive the information they need from the U.S. government to effectively manage cyber risks. Several recent legislative proposals, including CISPA, also seek to address this issue. While we recognize that recent events—namely, National Security Agency contractor Edward Snowden's disclosure of large quantities of classified information—will make policymakers more reluctant to increase the number of security clearances available, selective granting of security clearances to industry officials will play an important role in enabling the power sector to more effectively act on the government's threat information to protect the grid.

On the other hand, while access to threat information from the government is essential, utilities and other power sector companies—as the entities operating at the front line of cyber threats to the electric grid—may obtain data on some threats more quickly than the government. Given the difficulty of gaining access to classified data on cybersecurity threats, members of our advisory group noted that many companies have begun to develop their own operations to gather and analyze intelligence data and develop countermeasures.

Recommendations

- In accordance with Executive Order 13636, efforts to streamline the security clearance process for selected employees in the electricity sector should continue.
- At the same time, intelligence agencies should declassify relevant threat and vulnerability information as "for official use only" whenever possible. Agencies should leverage "tear line" and "share line" policies and procedures to facilitate sharing of portions of otherwise classified or restricted reports with private sector partners. Often, only a portion of the information collected in connection with a particular threat is classified, such as who the actors are and how the information was obtained. In this context, the sharing and distribution of threat information can be greatly facilitated by creating "tear lines" and separating classified information from unclassified information.
- The federal government should continue to support programs such as CRISP that facilitate machine-to-machine information sharing. This type of information sharing is critical given the speed at which cyber threats develop and propagate.
- Utility-led efforts to collect and share information on threats and vulnerabilities should be expanded and should complement information sharing between the government and industry. State PUCs and the federal government should continue to support these efforts.
- DHS, the ES-ISAC, and industry should consider how to most efficiently share threat and intelligence information with trusted vendors. Research and actions by vendors may be key to resolving vulnerabilities and mitigating the risk posed by individual threats, but vendors do not have direct access to information to enable timely research into how to best address these.

Support Information Sharing with International and State Counterparts

As discussed earlier, the North American electric grid is governed by multiple entities and its geographic span extends through the continental United States, Canada, and parts of Mexico. In the United States, the bulk power system is regulated at the federal level, while state PUCs oversee most distribution systems. Coordination among relevant entities in the United States, Canada, and Mexico, and among federal and state authorities is essential to mitigate the cyber risks facing the North American electric grid.

A number of efforts are already underway to improve information sharing between the United States and Canada, as well as between federal and state agencies. The ESCC, for example, has provided an opportunity to advance coordination between United States and Canadian government officials and to promote leadership from utilities in both countries. In addition, in October 2012, DHS and Public Safety Canada announced a Cybersecurity Action Plan to strengthen cybersecurity cooperation between the two countries. Among other things, the Action Plan calls for standard protocols for public-private information sharing.[134]

Finally, several pieces of proposed legislation in Congress have recognized the value and importance of expanding information sharing and broader engagement around combating cybersecurity threats with U.S. government partners. For example, the 2010 Grid Act required FERC to "consult with appropriate Canadian and Mexican authorities to develop protocols for the sharing of protected

information."[135] Likewise, international engagement is recognized as a fundamental component of the cybersecurity mission and public-private collaboration envisioned in the Cybersecurity Act of 2013.[136]

Recommendations

- The U.S. intelligence community, DHS, and DOE should conduct regular outreach to state PUCs, other relevant state agencies, and public and municipal utilities on cyber threats and vulnerabilities. These federal agencies could identify best practices for the focused sharing of classified information with public sector entities as needed to protect critical infrastructure.
- U.S. intelligence officials should conduct regular outreach and briefings, including classified briefings with relevant state officials and with Canadian and Mexican government and industry counterparts. DHS and DOE should also work to ensure that these counterparts are able to engage in all relevant government-industry forums, such as the newly reorganized ESCC.

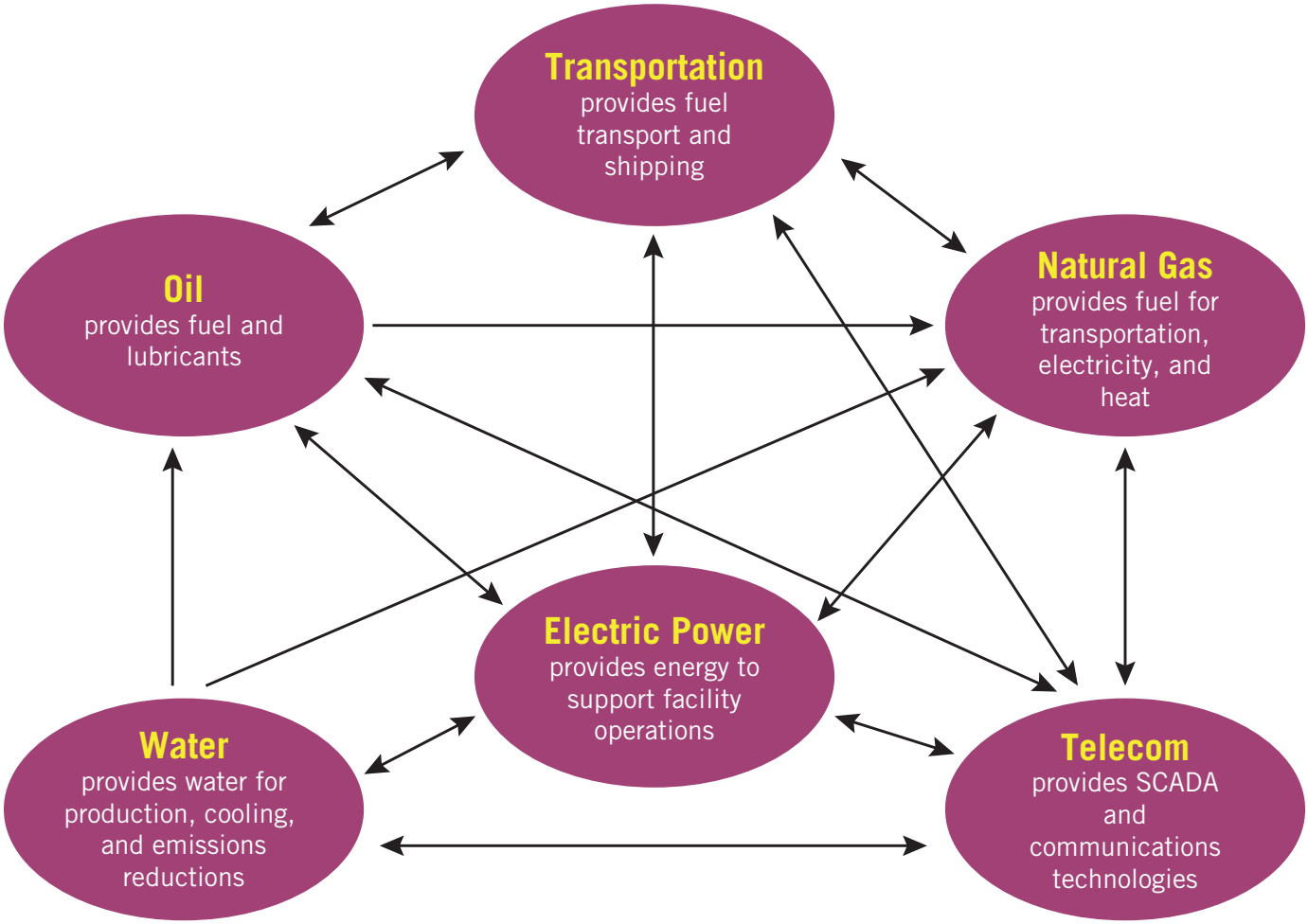
Support Information sharing across Critical Infrastructure Sectors

The operational performance of the U.S. electricity power system is inextricably linked to that of other critical infrastructure sectors that face similar cyber threats, including oil and natural gas, water, and telecommunications. (See Figure 3.) The power sector relies on telecommunications systems for grid operation, on pipelines to transport fuel, and on water systems to provide steam for generating power and to cool power plants. Each of these critical infrastructure sectors, in turn, relies on electricity for its operations. Mechanisms for quickly and securely sharing information across critical infrastructure sectors are critical for managing cyber risks.

Recommendations

- DHS should encourage organizational standardization across ISACs to promote a more efficient flow of information between the ISACs of various critical infrastructure sectors and the government.
- Mechanisms should also be developed to facilitate direct industry-to-industry information sharing (or company-to-company) communication. The DHS-supported Structured Threat Information Expression (STIX)[137] and Trusted Automated Exchange of Indicator Information (TAXII)[138] programs that are currently being developed with government and private-sector participation are examples. STIX is a collaborative, community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX language is intended to be sufficiently flexible and expressive to convey the full range of potential cyber threat information. TAXII is a program to enable sharing of actionable cyber threat information represented as STIX across organization and product/service boundaries.

Figure 3. Examples of Critical Infrastructure Interdependencies



Adapted from: Rinaldi, Peerenboom, and Kelly (2001)"Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies" IEEE Control Systems Magazine, December. Available at: http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 5: Responding to a Cyber Attack on the North American Electric Grid

A successful, large-scale cyber attack on the electric grid would likely present substantial technical, logistical, and coordination challenges. Cyber-specific responses, such as the removal of malware, would be required, along with more traditional disaster response operations to deal with the myriad consequences of a widespread loss of electric power—including, above all, threats to public health and safety resulting from the disruption of critical infrastructure and services. At the same time, law enforcement and intelligence agencies would need to investigate the cyber attack, both to identify, apprehend, and prosecute the perpetrators and to support efforts to prevent future attacks.

The appropriate actions to be taken by different government and industry entities in such an event will depend on the nature and origins of the attack and on how the attack manifests on and off the grid. In the early phases, it may not be possible to identify either the origins of an attack or its implications for the broader system. This heightens the need for efficient and ongoing communication between power sector entities and designated government agencies as security incidents develop. It also underscores the need for response models that specify a clear chain-of-command among government agencies but can also be quickly adapted as new information emerges. While Executive Order 13636 has helped clarify roles and responsibilities for cybersecurity within the U.S. government, significant questions remain concerning agency roles in the event of an attack on the North American electric grid.

This section discusses the different challenges that would arise in the event of a large-scale cyber attack on the electric grid, and provides a summary of the two existing response frameworks in the United States that would govern actions undertaken by private- and public-sector entities in the aftermath of such an attack. The first of these frameworks responds to the physical impacts of a prolonged and/or widespread power outage and would apply equally in the event of a natural disaster such as a hurricane.

The second specifically addresses the cyber aspects of an attack. We provide recommendations for improving both of these existing frameworks and for reconciling the differences that currently exist between them.

Understanding the Response Challenge

While some of the consequences of a large-scale cyber attack on the electric grid would be similar to those of any other event that disrupts electricity service—whether that event is a downed tree limb or a severe storm—restoring power after a successful cyber attack can be anticipated to pose additional challenges. Over the past few years, NERC and the electric power industry have sought to analyze and plan for these challenges. A recent NERC report identifies several specific aspects of a major cyber attack that could complicate restoration and recovery efforts:[139]

- The emergence of "unplanned" unstable islands;[140]
- Degradation of automatic response systems and automatic generation controls;
- Load shedding and prioritized restoration in a region- or interconnect-wide loss of power;
- Degradation and possible cyber manipulation of monitoring tools, data, etc.;
- Cyber risks to control centers;
- Disruption of communications and transportation infrastructure essential for restoration;
- Other intra-dependencies of electricity and other critical infrastructure; and
- Supply chain disruptions (especially the risk of physical damage to high voltage transformers and other key grid components).

Fortunately, existing response plans provide a sound foundation for preparing for a cyber attack. Based on lessons learned from Superstorm Sandy, many utilities and other companies with grid assets are working to strengthen their plans for operating in a disrupted environment, where some of the infrastructure essential to grid restoration—including communications and transportation services—are also affected.[141] That said, the disruptions associated with a large-scale cyber attack are likely to challenge utilities' operational abilities.

The range and variety of response operations that would likely be triggered by a severe cyber attack will complicate efforts to conduct these operations in an effective and integrated way, especially in a political environment that is likely to be challenging for government and industry authorities alike. One issue that will have to be addressed is the existence of two distinct and different frameworks for traditional versus cyber-specific response activities. Guidance for responding to traditional disasters is provided by the National Response Framework (NRF),[142] which was developed by DHS in 2008 and updated in 2010. A separate framework, developed by DHS in 2010 and known as the 2010 Interim National Cyber Incident Response Plan (NCIRP), is designed to guide response activities in the specific case of a cyber attack on critical infrastructure.[143] It is incumbent on policymakers to clarify how these two response systems can operate in a mutually supportive manner and to resolve ambiguities that may exist under the two frameworks with respect to roles, responsibilities, and authorities for federal agencies involved in response efforts.

The National Response Framework

The NRF provides well-established guidelines for traditional disaster-response operations, including the following:

- Fundamental, doctrinal principles to guide, structure, and integrate response efforts across all levels of government, and for government to coordinate with NGOs and private-sector partners.[144] In particular, the NRF is aligned closely with the National Incident Management System, which provides the incident management system on which the framework relies and specifies the command-and-control arrangements for disaster responders.[145]
- Specific emergency support functions and (together with the National Preparedness Goal) core capabilities required for each function, including transportation, communications, and energy.[146]
- Clear descriptions of the roles and responsibilities of federal departments and agencies, including the lead federal organization for each specific aspect of disaster response.[147]

The NRF has a strong statutory foundation. In particular, the Stafford Act provides "triggers" and thresholds for federal support activities and reimbursement mechanisms for disaster-response operations; in addition, it authorizes the federal government to conduct specific disaster-preparedness and -response activities.[148]

Nevertheless, as Superstorm Sandy demonstrated, the power restoration and emergency support functions needed to respond to a multistate, multi-week power outage must be further strengthened. Under the existing NRF, organizational arrangements for supporting emergency power and grid restoration proved to be inadequate during Sandy. In response, the Federal Emergency Management Agency (FEMA), its interagency partners, and the electric power industry established a National Power Restoration Task

Force to clarify support priorities, delivery mechanisms, and reimbursement authorities.[149] A report by the interagency Hurricane Sandy Rebuilding Task Force identified major shortfalls in the ability of wireless communications systems to support power restoration efforts.[150] This report and other post-Sandy reports have detailed a range of other improvements that are needed for future grid restoration efforts.[151] Implementing these measures is critical to achieving improved preparedness for all hazards.

Interim National Cyber Incident Response Plan

Response operations that are specifically designed to restore the grid in the event of a cyber attack fall under the purview of the NCIRP. The NCIRP establishes a "strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident."[152] As an interim document, the NRIRP represents a vital first step toward meeting the novel challenges of responding to a large-scale cyber attack. Yet, recent exercises have identified significant shortfalls and ambiguities in the NCIRP strategic framework. The National Level Exercise 2012,[153] which simulated a far-reaching cyber attack on SCADA networks and other critical infrastructure components, identified several key areas for improvement:

- Doctrinal and structural challenges, including time-consuming decision processes and an inability to generate viable, prioritized action plans;
- Problems in accessing certain critical capabilities, including an inability to provide or procure the technical resources necessary to meet requests for assistance;
- Ambiguities in the roles and responsibilities of various response agencies, including a lack of detail on the functions of response organizations; and
- Uncertainties over the statutory authority for federal assistance, including how the Stafford Act might authorize federal support activities and reimbursement efforts following a cyber attack.[154]

DHS, DOE, and other federal departments and agencies are partnering with other government agencies and private firms to address these general problems, as well as other specific problems associated with cyber attacks on the grid. For example, DHS has begun to collaborate with government and industry partners to draft a playbook for responding to destructive malware operations for the energy sector. This effort is aimed at providing a checklist of essential mitigation, response, and coordination tasks. A range of initiatives are also underway to strengthen the two-way flow of sensitive information on cyber attacks and mitigation efforts. Finally, DHS and DOE are working on an initiative to identify core capabilities for responding to cyber attacks on critical infrastructure and to build an incident action plan for preventing, protecting, mitigating, responding and recovering from such attacks.[155]

Resolving Differences between Response Frameworks

Differences and potential conflicts between the NRF and NCIRP could give rise to unnecessary debates and power struggles in the midst of a cyber attack, when clear lines of authority and coordinating mechanisms will be most vital. These differences will also complicate efforts to build a unified system of protocols for responding to cyber events that have associated physical impacts. Integrating cyber and traditional disaster-response systems will be vital to save lives and limit the damage associated with an effective attack on the North American electric grid.

Both existing response frameworks recognize the need for coordination to deal with cyber disruptions and their

physical consequences. Noting that "cyber attacks can have catastrophic physical consequences," the NRF is intended to provide guidance for response operations in all types of disasters.[156] The NCIRP, in turn, emphasizes that it was intended to "build on the foundations of the NRF" and "facilitate the coordination with NRF mechanisms during cyber incidents with physical consequences."[157] Nevertheless, on issues that are vital for conducting and coordinating response operations, important distinctions exist between the NRF and NCIRP. In particular, the frameworks differ in the following key areas:

- *Chains-of-command, coordinating mechanisms, and protocols for government and industry interaction.* For example, under the National Response Framework, the Emergency Support Function system provides the primary means for building, sustaining, and delivering core response capabilities across the federal government.[158] The NCIRP relies on separate mechanisms to coordinate cyber-response efforts, including the NCCIC and the Cyber Unified Coordination Group's Incident Management Team.[159]
- *Thresholds for federal assistance and other federal activities.* For the National Response Framework, the Stafford Act provides specific triggers for federal assistance (including the declaration of emergencies and major disasters).[160] The NCIRP rests on an entirely different set of thresholds provided by the National Cyber Risk Alert Level (NCRAL) system.[161]

Most important, the two frameworks make different assumptions concerning the roles and responsibilities of state governors. Under the NRF, governors are at the heart of the process for requesting federal assistance and for engaging other response mechanisms.[162] More broadly, the NRF recognizes that states are sovereign entities and that governors bear primary responsibility for public safety in their states.[163] The NCIRP specifies no remotely equivalent role for governors, even though a severe cyber attack could jeopardize the lives of citizens as much or more than any hurricane.

While it is necessary to reconcile the kinds of fundamental differences in authorities and protocols that currently characterize the NRF and NCIRP, a single response framework would not be adequate to cover the range of situations that could arise. In the event of a cyber attack, response efforts will need to include some cyber-specific features or operations—such as eradicating malware—that would not be relevant in the event of a natural disaster. The NCIRP makes an important contribution as it provides a foundation upon which to build these cyber-specific protocols.

Finally, given that a cyber attack on the grid could have implications and impacts that cross international borders, any response framework must consider how response coordination and sharing of information with relevant international government and industry counterparts will be executed.

Recommendations

- While the NCIRP represents a crucial first step, federal policymakers should take several additional actions to strengthen the governance and coordination framework for cyber event response:

  - Clarify and further develop the chain-of-command and decision-making mechanisms among federal agencies, and among the federal government and state and local governments, as well as international counterparts, where appropriate.
  - Clarify the roles and responsibilities of individual government agencies, and resolve areas of overlapping responsibility.

- Strengthen protocols and concepts of operation for government and industry interaction and mutual support.
- Clarify thresholds that would trigger federal government involvement, and specify the conditions under which authorities granted by the Stafford Act would apply in the wake of a cyber event.
- Further develop the NCRAL system to clarify the conditions that would lead to a change in the NCRAL alert level, as well as the activities that should occur at each level.
- Update information sharing protocols to improve timeliness. For example, improved tear line procedures and better coordination among agencies with relevant information could expedite the release of information.
- Better define the roles, responsibilities, and authorities of the Unified Coordination Group (UCG). The UCG is the interagency and inter-organizational coordinating and decision-making body that plays a critical role in executing the NCRIP.

- The existing cyber-response system not only needs to be improved; it needs to be better integrated into the broader response effort—governed by the NRF—that a severe cyber attack on the grid would require. In particular, the NCIRP should be updated to provide an elevated role for governors analogous to their role in the NRF. Governors—by virtue of being in closer proximity to citizens and businesses in their states—have a better understanding of assistance needs at the local level than the federal government. For this reason, governors should have a clearly defined role in working with the federal government to request and guide federal relief. Assignment of state roles in the recovery effort should consider the possibility that ongoing cyber attacks after an initial event are unlikely to respect state boundaries—remaining vulnerabilities in one state may have implications for a broader region. More generally, improved integration between the NRF and NCIRP is needed across their respective chains-of-command, coordinating mechanisms, and thresholds for providing federal assistance.
- Governors should further strengthen state-wide governance structures for cyber preparedness. The National Governors Association has proposed that state chief information security officers be given stronger responsibilities and authorities to coordinate state action.[164] For cyber events responses that involve both cyber-specific and physical consequence management efforts, however, state emergency management and public safety leaders will also play key coordination roles (and will directly support governors for NRF-related coordination with FEMA).[165]
- Response protocols should provide clarity on the respective roles and responsibilities of law enforcement who are seeking to preserve information for criminal investigations and public- and private-sector responders seeking to reestablish critical services.
- Federal agencies, state agencies, and critical infrastructure sector participants should continue to conduct scenario exercises such as the National Level Exercise to practice response protocols for large-scale cyber attacks. Such exercises are critical for building relationships between key actors, improving efficiency in exercising protocols, and identifying gaps in existing protocols.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 6: Paying for Electric Grid Cybersecurity

A recent study estimates that U.S. utilities will spend about $7 billion on cybersecurity by 2020.[166] An important issue for policymakers, state regulators, and utilities as they take steps to minimize the grid's exposure to cyber threats concerns the distribution of costs associated with these investments between utility shareholders and customers. Owners of grid infrastructure differ in their abilities to recover the costs of investments in these assets. Some entities will be able to seek cost recovery through FERC-approved tariffs; other entities, like investor-owned distribution utilities, may be able to seek cost recovery through state-approved rate schedules. Public utilities and rural cooperatives can generally pass costs on to ratepayers, though they are commonly under pressure to limit rate increases. Meanwhile, other entities, such as wholesale power generators, do not have cost-of-service rates or monopoly customers; for these entities, the ability to recover costs incurred to improve cybersecurity may depend on contract terms and market conditions.

In a cost-of-service environment, regulators may lack the tools or expertise to identify whether a particular investment is prudent or whether investments that are critical to the system are being overlooked. In addition, regulators are likely to have difficulty weighing the costs and benefits of individual investments, as cybersecurity benefits are difficult to quantify and include public as well as private benefits that may be difficult to separate. Another challenge in a cost-of-service environment is that as utilities face pressure to make significant investments in cybersecurity and other areas of grid modernization, many are doing so in an environment of slow or, in some cases, declining load growth. Utilities typically face a lag between capital expenditures and cost recovery, which may negatively affect cash flows. This lag, when combined with slow-growing or declining sales, may impair utility earnings and deter them from making potentially beneficial capital investments.[167]

This section discusses some of the challenges that regulators face when evaluating utility investments in cybersecurity for cost-recovery purposes. Some of these challenges flow from the "public good" nature of many cybersecurity investments, particularly where there are systemic risks involved and a utility's ability to finance investments or pass costs through to ratepayers is limited.

Evaluating Cybersecurity Investments for Cost Recovery

State utility regulators play a key role in advancing electric grid cybersecurity, particularly through their approval of utility expenditures. However, regulators face a number of challenges when evaluating cybersecurity investments. First, information asymmetries limit a commission's ability to fully evaluate the cybersecurity options or needs of an individual utility. Regulatory commissions generally do not have personnel at utility sites and typically are not in a position to observe what investments the utility decides not to pursue. A commission can only decide cases based on the record presented. If a utility's cybersecurity strategy overlooks particular investments in favor of others, the inherent trade-offs in terms of costs and benefits may not be described in a commission's proceedings.

Second, limited experience with cyber threats and cybersecurity makes it difficult for commissions to evaluate utility programs in this area. Few public utility commissioners have experience with the management of information and control systems. In fact, many commissioners come from outside the utility industry and face a more basic learning curve in understanding electric utility operations generally. Finally, commission staffs generally have limited cybersecurity experience and education.

Third, evaluating investments in cybersecurity is challenging because the benefits of these investments are difficult to quantify and may extend beyond an individual utility to the broader grid and even to the broader economy. Further, the novelty and evolving nature of cyber risks

makes it difficult—even for experts—to evaluate the benefits of potential security investments. The challenges inherent in quantifying cybersecurity benefits—e.g., what is the probability of a cyber event absent a particular investment, and what are the costs of that event?—mean that cybersecurity benefits may receive only qualitative consideration. The cost-benefit analyses used in regulatory proceedings are generally not designed to address risk and uncertainty. Benefits that involve risk and uncertainty, or that are difficult to quantify, may carry less weight when compared with clearly identifiable utility costs.

NARUC has been working to address some of these challenges, through both direct outreach and the preparation of cybersecurity guidance for state PUCs. This guidance provides regulators with insights into how to develop a strategy for addressing utility cybersecurity and offers specific questions that regulators can use in their dialogues with utilities.[168]

"Public Good" Nature of Cybersecurity Investments

Cyber vulnerabilities in the power system can create systemic risks. Past blackout events have illustrated the extent to which failures at a single entity can have widespread ramifications. The 2003 Northeast blackout, for example, originated at facilities in Ohio and affected more than 50 million people in the United States and Canada. It cost the U.S. economy an estimated $6 billion.[169] While the blackout was not linked to malicious activity and had multiple causes, analysis of the event concluded that a failure in a software program may have played a significant role in the outage.[170] A small utility with limited resources could own or operate a critical facility, which—if disrupted—could trigger a large regional outage. A cyber attack on a customer or third-party generator could have consequences that flow through the grid to impact other customers or utilities.[171] Moreover, electricity is needed to power gas and oil pipelines, water systems, telecommunications, and other critical infrastructure. An extended power outage could have significant spillover impacts.

To the extent that the benefits of cybersecurity investments (or, conversely, the costs of a cyber attack) extend beyond an individual company, that company may invest at a level that is less than optimal from the perspective of the system as a whole. The regulatory process is also likely to overlook systemic risks. State regulators typically decide cases on a utility-by-utility basis. These factors will tend to limit the visibility of systemic risks in regulatory proceedings.

Individual systems or facilities vary in the extent to which their loss would affect a larger portion of the grid—in other words, some facilities could be deemed more "critical" than others. That said, defining the criticality of an individual facility is a challenge, because the relative importance of that facility may change depending on the timing and nature of the cyber event, as well as over the course of the event as it unfolds. Despite this challenge, we believe the institute described in Chapter 3 could play an important role in evaluating sources of systemic risk on the grid, and—with the help of participating entities—identify assets that, because of their criticality to the system, may warrant greater investments in cybersecurity.[172] While such analysis can help guide investments, it does not resolve the challenging question of how the costs of such investments should be allocated, particularly given that the benefits of these investments may largely occur outside an individual entity's footprint. Addressing the costs of cybersecurity investments at small entities or entities that are operating in competitive markets should be a concern for policymakers and the industry as a whole, because a lack of resources or an inability to recover costs could otherwise deter these entities from making broadly beneficial investments.

In fact, the case for congressional action in the area of electric system cybersecurity is perhaps nowhere more compelling than with respect to the public good nature of electric grid cybersecurity investments. The cyber and physical threats facing the electric grid mean that the

actions of utilities and other grid asset owners and operators have implications for national security. A secure power sector infrastructure is essential not only to the economy broadly, but also to the provision of other critical services (like water, communications, public safety, and health). There is a clear role for Congress to play in considering how the costs of cybersecurity investments with broad system benefits should be paid for, as well as in providing funding to ensure continued innovation in tools and technologies that advance cybersecurity.

Recommendations

- DOE should fund efforts—to be undertaken via the institute described in Chapter 3 and in collaboration with utilities, state regulators, and system operators—to fully evaluate and understand systemic cyber risks, including risks involving interdependencies and the spillover of consequences from one entity or jurisdiction to another. Such analyses would help utilities and regulators alike identify investments that are critical to the system as a whole. DOE should also fund research on the value of uninterrupted service to help regulators better evaluate the potential impacts of cyber attacks and provide needed context for weighing the benefits of utility investments in cybersecurity.
- State regulators should support efforts to establish the institute described in Chapter 3 and develop a plan for continued engagement with this organization. The institute's work could help normalize cybersecurity best practices for utilities and provide regulators with greater confidence in making cost-recovery decisions and evaluating utility governance and risk-management approaches.
- State and federal regulators should proactively engage with companies to establish priorities and needs that companies have for improving their cybersecurity postures. Where possible, this can be undertaken outside of a docketed proceeding to minimize the risk of broadly disclosing vulnerabilities.
- DOE should work with industry and with NARUC to develop metrics that would be useful for evaluating utility investments in cybersecurity. One can envision alternative approaches, including: compliance with NERC CIP standards and the requirements established by the institute, metrics related to voluntary disclosures to the ES-ISAC, achievement of specified ES-C2M2 maturity levels, independent audits, and/or third party penetration testing results.
- State and federal regulators should evaluate cost recovery for cybersecurity investments against the metrics developed under the initiatives described above.
- Given the adaptive nature of cyber threats, and the challenges associated with encouraging new investments under cost-of-service regulation when sales growth is slow or declining, the regulatory approach taken should encourage continuously improving cyber capabilities. This may mean applying something other than a reasonable or unreasonable (pass/fail) test. For example, one alternative regulatory model could be to match the level of regulatory scrutiny to performance on specified cybersecurity metrics. A second option could be to devise forward-looking regulatory contracts with financial incentives, both for performance on cybersecurity metrics and cost efficiency in achieving those outcomes.
- Policymakers and industry should consider alternatives for providing support to entities that own critical assets but may lack the resources or be unable to recover costs for needed cybersecurity improvements. One option would be to establish a fund at the institute that would provide assistance to entities in these cases so that they could make the cybersecurity investments recommended by the institute. DOE could provide seed money for this fund in the early years of the institute's operation.
- DOE should continue to support cybersecurity research and development to advance cybersecurity tools and capabilities. Congress should continue to provide resources to enable this support.

■ **Energy & Infrastructure Program**
Energy Project

■ **National Security Program**
Homeland Security Project

Chapter 7: Conclusion

New polices and public-private partnerships are needed to address the growing threat of cyber attacks on the North American electric grid. These approaches must enlist the respective capabilities and strengths of government and private sector actors, promote effective risk-management strategies that can evolve in response to the changing nature of cyber threats, and work to limit the costs of any successful attacks. Power sector companies need tools and incentives that will enable them to invest in cybersecurity in ways that benefit the broader system and to support the development of advanced cybersecurity solutions. All stakeholders should also work together to foster rapid information sharing and improved situational awareness across government authorities and power sector companies, prepare and test response protocols to plan for possible conditions under worst-case-scenario events, and determine how the costs of managing cybersecurity risks will be allocated.

Efforts to spur socially optimal levels of investment in grid cybersecurity are complicated by the sheer diversity and number of entities involved in the power sector and by the public good nature of many cybersecurity investments. More than 3,200 individual companies and organizations play a role in the generation, transmission, and distribution of electricity across the electric grid. Numerous vendors supply the software and advanced grid technologies that are laying the foundation for a modernized grid, which, despite its many benefits also implies new sources of vulnerability and an increasingly complex supply chain. At the same time, because of the interconnected nature of the grid, individual entities are unlikely to fully capture the benefits of their own cybersecurity investments. Finally, the electric sector is intricately connected to other critical infrastructure sectors—as a result, the operational consequences of a successful cyber attack on the grid could propagate quickly across the economy, with rapidly escalating costs.

Given the complexity of the electric power system and the overlapping roles of numerous federal, state, and local agencies involved in some aspect of grid cybersecurity and event response, this Initiative has sought to develop policy recommendations that help clarify the responsibilities of different entities and identify gaps where additional policies are needed. With the help of the Initiative's advisory board, we, the co-chairs of this project, have identified a number of opportunities to advance cybersecurity standards and practices, promote information sharing, improve response preparation, and address cost recovery. The recommendations in these areas target Congress, federal government agencies, state PUCs, and industry.

As noted throughout this report, the electric power industry and the government agencies that oversee it have already done much to improve grid cybersecurity. The bulk power system and nuclear power plants, in particular, are already subject to mandatory cybersecurity standards. In addition, extensive collaboration on cyber risks has occurred within the industry and via public-private partnerships with a range of government entities. However, it is also clear that existing policies and practices suffer from limitations that must be overcome to more effectively manage ever-evolving cyber threats. The recommendations in this report target several key priorities for managing cyber risks across the grid:

- The development of an industry-wide organization—modeled after the nuclear power industry's highly successful INPO—to advance cybersecurity throughout the electric power sector. This organization would complement the mandatory standards that already exist for the bulk power system and would seek to advance cybersecurity across all components of the electric grid.
- More efficient sharing of actionable information on cybersecurity threats and vulnerabilities along a number of dimensions, including between industry and government, within industry and across critical infrastructure industries, and among government

entities. In particular, steps must be taken to ensure that industry can share information with government without fear of compliance actions or liability. At the same time, government agencies must identify ways to quickly declassify and share threat information with power sector officials.

- The development of improved response protocols for cyber and coordinated cyber-physical attacks. Such protocols must clearly define the roles and responsibilities of different government agencies, clarify thresholds for federal involvement, and ensure a strong role for governors. Response protocols should be exercised frequently.
- Funding for the analyses needed to identify and understand major sources of systemic risk from cyber attacks, the development of cybersecurity tools and practices that can be easily adopted by multiple electric power sector entities, and the development of metrics against which to evaluate utility investments in cybersecurity.

In the coming months, BPC staff and Initiative co-chairs will reach out to policymakers and stakeholders to advance these and other recommendations. At the same time, BPC will work to address challenges that would remain even if all the recommendations in this report were adopted. For example, because privacy concerns continue to present a stumbling block for efforts to enhance information sharing between industry and government, additional ideas and compromises will be needed to break the current legislative logjam in this area. Going forward, BPC's Homeland Security Project will explore further options to address these challenges. In the coming months, BPC's Energy Project plans to address the broader issue of electric grid resilience, including the role and potential benefits of modern grid technologies and practices in addressing multiple threats (e.g., weather, physical, cyber, geomagnetic) to the grid.

Endnotes

1. Reuters, "FBI: Cyber-attacks Surpassing Terrorism as Major Domestic Threat," November 14. Available at: http://rt.com/usa/fbi-cyber-attack-threat-739/.
2. U.S. Department of Homeland Security (2013) "Incident Response Activity," ICS-CERT Monitor. April-June. Available at: http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf.
3. See, for example,Dlouhy, Jennifer A. (2013) "Utility Executives: Major Cyberattack on Power Grid is Inevitable," August 6, *Fuel Fix*. Available at: http://fuelfix.com/blog/2013/08/06/utility-executives-major-cyberattack-on-power-grid-is-inevitable/.
4. The U.S. Department of Energy estimated costs of $6 billion, a figure that is near the $6.4 billion mid-range estimate prepared by Anderson Economic Group. For a summary of estimates of the blackout's costs, see: Electric Consumers Resource Council (2004) *The Economic Impacts of the August 2003 Blackout*, February 9.
5. National Academy of Sciences (2012) *Terrorism and the Electric Power Delivery System*. Available at: http://www.nap.edu/catalog.php?record_id=12050.
6. North American Electric Reliability Corporation (2013) 2013 *Long-Term Reliability Assessment*, December. Available at: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2013_LTRA_FINAL.pdf.
7. U.S. Government Accountability Office (2012) *Cybersecurity: Challenges in Securing the Electric Grid*, p. 9.
8. U.S. Government Accountability Office (2012).
9. Massachusetts Institute of Technology Energy Initiative (2011) *The Future of the Electric Grid*, p. 212.
10. Nuclear power facilities are also subject to enforceable cybersecurity standards.
11. In particular, building on an incident action plan known as "Energizer," the DHS, in conjunction with the DOE and the Electricity Subsector Coordinating Council , is developing a coordinated response that leverages both government and industry assets and capabilities. See Serbu, Jared (2013). "DHS Building Actionable Response Plans for Cyber Attacks on Critical Infrastructure." *Federal News Radio*, August 8. http://www.federalnewsradio.com/index.php?nid=851&sid=3415445.
12. Exec. Order No. 13,636, 78. Fed. Reg. 11,739 (Feb. 19, 2013) at § 4(a).
13. *Id*. at § 9(a) and § 5(b).
14. *Id*. at § 7(a).
15. National Institute of Standards and Technology (2014) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.* Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
16. *Ibid*., p. 1.
17. Suchman, Bonnie (2013) *Addressing Liability Issues for Electric Utilities*. EUCI Electric Utility Cybersecurity Conference. October, 9: Washington, D.C.
18. Testimony of David A. Whiteley, executive vice president of NERC (2007) *The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid*, October 17.
19. Order 706 (2008) 122 FERC 61,040; Notice of Proposed Rulemaking (2013) *Version 5 Critical Infrastructure Protection Reliability Standards*, 143 FERC 61,055.
20. North American Electric Reliability Corporation. About Alerts. Available at: http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx.
21. Electricity Sector Information Sharing and Analysis Center. Available at: http://www.esisac.com/SitePages/Home.aspx.
22. The full set of activities undertaken by the ES-ISAC is described at: http://www.esisac.com/SitePages/Home.aspx.
23. North American Electric Reliability Corporation. GridEx. Available at: http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.
24. North American Electric Reliability Corporation. GridSecCon. Available at: http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx.
25. U.S. Department of Homeland Security and U.S. Department of Energy (2010) *Energy Sector-Specific Plan. An Annex to the National Infrastructure Protection Plan*. Available at: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.
26. See U.S. Department of Energy, *Energy Delivery Systems Cybersecurity*. Available at: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity.
27. U.S. Department of Energy (2013) "Energy Department Announces New Investments of over $30 million to Better Protect the Nation's Critical Infrastructure from Cyber Attack." September 19. Available at: http://energy.gov/articles/energy-department-announces-new-investments-over-30-million-better-protect-nation-s.
28. Energy Sector Control Systems Working Group (2011) *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September. Available at: http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.
29. U.S. Department of Energy, *Energy Delivery Systems Cybersecurity*. Available at: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity.
30. U.S. Department of Energy and U.S. Department of Homeland Security (2012) Electricity Sector Cybersecurity Capability Maturity Model(ES-C2M2) version 1.0, May. Available at: http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf.
31. *Ibid*.
32. U.S. Department of Energy, Cybersecurity Risk Management Process (RMP). Available at: http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp.
33. U.S. Department of Homeland Security, About the National Cybersecurity Communications Integration Center. Available at: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.
34. U.S. Department of Homeland Security, The Industrial Control Systems Cyber Emergency Response Team. Available at: http://ics-cert.us-cert.gov/.
35. U.S. Department of Homeland Security, *Cyberstorm: Securing Cyber Space*. Online. Available at: http://www.dhs.gov/cyber-storm-securing-cyber-space.
36. National Institute of Standards and Technology (2010) *Interagency Report (IR) 7628. Guidelines for Smart Grid Cybersecurity*, September. Available at: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.
37. National Institute of Standards and Technology (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.*
38. H.R. 624, 113th Cong. (1st Sess. 2013).
39. H.R. 624, 113th Cong. (1st Sess. 2013).
40. H.R. 756, 113th Cong. (1st Sess. 2013).
41. S. 1353, 113th Cong. (1st Sess. 2013).
42. S. 3414, 112th Cong. (2d Sess. 2012).
43. Most electric cooperatives and publicly owned utilities, which serve the remaining customers, are not regulated by state commissions or are regulated in only limited circumstances, such as for facility siting and in declared emergencies.
44. For FERC-jurisdictional activities, states must pass through costs deemed prudent by FERC.
45. National Association of Regulatory Utility Commissioners (2010) *Resolution Regarding Cybersecurity*, February. Available at: http://www.naruc.org/Resolutions/Resolution%20on%20Cybersecurity1.pdf.

46. National Association of Regulatory Utility Commissioners (2013) *Resolution Regarding Cybersecurity Awareness and Initiatives*, August. Available at: http://www.naruc.org/Resolutions/Resolution%20Regarding%20Cybersecurity%20Awareness%20and%20Initiatives%20CI.pdf.
47. Keogh, Miles, and Christina Cody (2013) *Cybersecurity for State Regulators 2.0, with Sample Questons for Regulators to Ask Utilities*. NARUC. Available at: http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf.
48. 52 Pennsylvania Code Chapter 101.
49. PUC SUBST. R. §25.130. Available at: http://www.puc.state.tx.us/agency/rulesnlaws/subrules/electric/25.130/25.130.pdf.
50. PUCT (2012) Project 40128: *Report on Electric Grid Cybersecurity in Texas*, November.
51. Chairman Todd A. Snitchler (2012) *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources, Full Committee Hearing on Cybersecurity*, July 17 (hereafter: Snitchler); see also: Thomas Pearce, *Cybersecurity and Regulators*, NESCO Guest Blog. Available at: http://www.us-nesco.org/guest-blog/public-utility-commission-of-ohios-thomas-pearce-on-cybersecurity-and-regulators/.
52. Snitchler at p. 9; See also: FERC (2008) *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC 61,040, January 18.
53. Snitchler at p. 9.
54. *Ibid*.
55. Washington Utilities and Transportation Commission (2013) *Discussion Draft of Cybersecurity Information Reporting Guidelines*, November 4, Docket U-131799.
56. National Governors Association (2012) "Governors O'Malley and Snyder to Lead NGA Resource Center on Cybersecurity," October 2. Available at: http://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html.
57. Public Safety Canada. *About Public Safety Canada*. Available at: http://www.publicsafety.gc.ca/cnt/bt/index-eng.aspx#prtfl
58. Public Safety Canada (2010) *Canada's Cybersecurity Strategy: For a Stronger and More Prosperous Canada*. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.
59. Public Safety Canada. *Action Plan for Critical Infrastructure*. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx#aB.
60. Declaration by President Obama and Prime Minister Harper of Canada (2011) *Beyond the Border*, February 4. Available at: http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord.
61. Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf
62. The Government of Canada does include a National Energy Board and a federal Ministry of Natural Resources; however, their mandates with respect to the electricity sector and cyberspace are quite limited and do not mirror those of FERC and DOE.
63. See: North American Electric Reliability Corporation (2013) *2012 Annual Report*, March. Available at: http://www.nerc.com/files/NERC%202012%20Annual%20Report%20(MAR13).pdf.
64. North American Electric Reliability Corporation, *Electricity Sub-sector Coordinating Council*. Available at: http://www.nerc.com/pa/CI/Pages/ESCC.aspx.
65. See: Smith, Michael (2013) *Improving Grid Resilience*. November 12. Available at: http://www.pjm.com/~/media/committees-groups/stakeholder-meetings/grid-2020-focus-on-resiliency/presentations/smith-presentation.ashx.
66. American Public Power Association (2012) *Cybersecurity Essentials—A Public Power Primer*. Available at: https://ebiz.publicpower.org/APPAEbiz/ProductCatalog/Product.aspx?ID=4909.
67. National Rural Electric Cooperative Association and Cooperative Research Network (2011) *Guide to Developing a Cyber Security and Risk Management Plan*. Available at: http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf.
68. Edison Electric Institute (2013) Electric Power Industry Initiatives to Protect the Nation's Grid from Cyber Threats, January. Available at: http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
69. Office of the Auditor General of Canada (2012) *Report of the Auditor General of Canada to the House of Commons*, Chapter 3: "Protecting Canadian Critical Infrastructure Against Cyber Threats." Available at: http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.
70. 16 USC. § 824o(c).
71. North American Electric Reliability Corporation (2006) 116 FERC 61,062 (ERO Certification Order), order on rehearing & compliance; 117 FERC 61,126 (ERO Rehearing Order) (2006), appeal docket sub nom. *Alcoa, Inc. v. FERC*, No. 06-1426, D.C. Cir. December 29.
72. Existing standards categories include Resource and Demand Balancing; Critical Infrastructure Protection; Communications; Emergency Preparedness and Operations; Interchange Scheduling and Coordination; Interconnection Reliability Operations and Coordination; Modeling, Data, and Analysis; Nuclear; Personnel Performance, Training, and Qualifications; Protection and Control; Transmission Operations; Transmission Planning; and Voltage and Reactive. See: NERC, United States Mandatory Standards Subject to Enforcement. Available at: http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United States.
73. Order 706, 122 FERC 61,040 (2008).
74. Order 706, 122 FERC 61,040 (2008).
75. See, for example, Statement of Representative Henry A. Waxman (2013) Hearing on Cyber Threats and Security Solutions, Committee on Energy and Commerce, May 21.
76. A specific example helps illustrate the concern about compliance risk: Currently, NERC CIP standards require a narrow assessment of vulnerability scanning. If an entity adopts a broader-spectrum scanning assessment and detects more vulnerabilities as a result, the entity would have increased its risk of registering potential violations. Since each of these potential violations must be processed through a NERC and FERC enforcement mechanism, the entity—by adopting a more robust internal compliance program than the minimum required by current standard—increases its exposure to civil penalties. In other words, the current system creates incentives for responsible entities to include in their compliance programs only the minimal "baseline" actions required by mandatory standards.
77. Order No. 791 (2013) *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 FERC 61,160, November 22.
78. U.S. Energy Information Administration (2012) *State Electricity Profiles 2010*, DOE/EIA-0348(01)/2, January. Available at: http://www.eia.gov/electricity/state/pdf/sep2010.pdf.

79. H.R. 5206, 111th Cong. (2nd Sess. 2010). The Act defined "defense critical electric infrastructure" as infrastructure in the United States used for the generation, transmission, and distribution of electricity that is (a) not part of the bulk electric system and (b) serves a facility designated by the president as critical for national defense.
80. S. 1342, 112th Cong. (1st Sess. 2011). "Critical electric infrastructure" was defined as infrastructure "so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety."
81. U.A. Government Accountability Office (2012) *Cybersecurity: Challenges in Securing the Electricity Grid*, Statement of Gregory C. Wilshusen, director, Information Security Issues. Testimony before the Committee on Energy and Natural Resources, U.S. Senate, July 17.
82. U.S. Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Program*. Available at: http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model.
83. National Electric Sector Cybersecurity Organization. Available at: http://www.us-nesco.org/. NESCO aims to "lead a broad-based, public-private partnership to improve electric-sector energy systems cybersecurity and become the security voice of the electric industry."
84. Report of The President's Commission on the Accident at Three Mile Island (1979) *The Need for Change: the Legacy of TMI*, June.
85. See, for example, discussion of INPO in National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011) *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling*, report to the president.
86. Testimony of Dr. Zack Pate, Former INPO CEO (2010) Before the National Commission on the BP Deepwater Horizon Oil Pill and Offshore Drilling, August 25.
87. *Ibid.*
88. *Ibid.*
89. Testimony of James O. Ellis, Jr., INPO CEO (2010) Before the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, August 25; Pate Testimony.
90. Note that many of these incentives are alluded to in a recent White House blog post summarizing potential incentives for participation in the Cybersecurity Framework. Daniel, Michael (2013) *Incentives to Support Adoption of the Cybersecurity Framework*, August 6. Available at: http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
91. Suchman (2013) "Ordinary negligence" is a common law standard consistent with reasonable care by a defendant to prevent injury.
92. *Ibid.*
93. U.S. Department of Homeland Security (2012) *Cybersecurity Insurance Readout Report*. Available at: http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.
94. *Ibid.*
95. *Ibid.*
96. *Ibid.*
97. *Ibid.*
98. *Ibid.*
99. *Ibid.*
100. Daniel (2013).
101. U.S. Department of Homeland Security (2012).
102. It is important to note that legislation designed in the manner of TRIA would impose budgetary costs in terms of the expected payout that would occur under the terms/duration of the act net of recoupment. Other models, such as the United Kingdom's financial backing of terrorism risk insurance pools, might pose less risk to taxpayers. See Congressional Budget Office (2005) *Federal Terrorism Reinsurance: An Update*. Available at: http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/60xx/doc6049/01-05-terrorism.pdf.
103. See, for example, Whitney, Lance (2011) "U.S. Warns of Security Holes in Chinese SCADA Apps," CNET, June 17. Available at: http://news.cnet.com/8301-1009_3-20072003-83/u.s-warns-of-security-holes-in-chinese-scada-apps/.
104. Available at: http://energy.gov/oe/national-scada-test-bed.
105. See: "Smart Grid Interoperatbility Panel." Available at: http://www.sgip.org/#sthash.vLm6aTmG.dpbs. See also: "Underwriters Laboratories." Available at: http://www.ul.com/global/eng/pages/.
106. National Institute of Standards and Technology (2013) *Preliminary Cybersecurity Framework*, p. 36.
107. *Ibid.*, p. 37.
108. PR Newswire, "New Industrial Control Systems Cyber Security Certification in Development." Available at: http://www.prnewswire.com/news-releases/new-industrial-control-systems-cyber-security-certification-in-development-223462451.html.
109. Global Industrial Cyber Security Professional, Global Industrial Cyber Security Professional. Available at: https://www.giac.org/promo/gicsp-special?utm_source=offsite&utm_medium=text-ad&utm_content=PR_GICSP_announce_9122013&utm_campaign=GIAC_Certification&ref=139030.
110. S. 1353, 113th Cong. (1st Sess. 2013).
111. NERC senior management indicated that they are unaware of any case where information shared with the ES-ISAC has led to compliance or enforcement actions. However, participants in our advisory group noted that concerns over the risk of such action – particularly among corporate counsel – have led them to withhold information from the ES-ISAC.
112. North American Electric Reliability Corporation (2013) *Policy on the Role of the Electricity Sector—Information and Analysis Center (ES-ISAC) vis-a-vis NERC's Compliance Monitoring and Enforcement Program*, March 8. Available at: http://www.nerc.com/files/Updated%20ES-ISAC%20Firewall%20Approval%20(13%20Mar%202013).pdf.
113. Letter from Patricia Hoffman, assistant secretary, DOE Office of Electricity Delivery and Energy Reliability, to Gerry Cauley, president and CEO, NERC, March 14, 2013. Available at: http://www.nerc.com/news/Headlines%20DL/ES-ISAC%20Letter%2014MAR13.pdf.
114. See, for example, American Civil Liberties Union, *CISPA Explainer*. Available at: https://www.aclu.org/blog/tag/cispa-explainer.
115. U.S. Department of Energy (2010) *Data Access and Privacy Issues Related to Smart Grid Technologies 17*, October 5. Available at: http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.
116. Mark F. Foley (2008) "Data Privacy and Security Issues for Advanced Metering Systems (Part 2)," *SmartGrid News*, July 1. Available at: http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html. See also: Federal Trade Commission (2013) *Protecting Consumer Privacy*. Available at: http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last updated July 16, 2013).

117. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2522).
118. Mark F. Foley (2008).
119. Liu et al. (2013) "Cybersecurity : Selected Legal Issues,"CRS Report R42409, April.
120. July 2, 1890, ch. 647, 26 Stat. 209 (codified at 15 USC. §§ 1-7).
121. 15 USC. § 1. ("Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal.")
122. See Federal Trade Commission and U.S. Department ofJustice (2000) *Antitrust Guidelines for Collaborations Among Competitors*. Available at: http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf (hereinafter "Competitor Collaboration Guidelines").
123. Letter from Joel I. Klein, assistant attorney general, DOJ Antitrust Division, to Barbara Greenspan, Esq., associate general counsel, Electric Power Research Institute, Inc., October 2, 2000. Available at: http://www.justice.gov/atr/public/busreview/6614.pdf.
124. *Ibid*.
125. In particular, the DOJ's letter expressly does not bind the DOJ beyond the date of its issuance in 2000 and does not apply to any program other than EPRI's information exchange. Further, it does not bind *private* litigants proceeding under the federal antitrust laws, and it does not affect any state competition law.
126. See Eric A. Fischer (2013) *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions 23-24*, Cong. Research Service. See also: Critical Infrastructure Information Security Act of 2001, S. 1456 § 7, 107th Cong. (expressly limiting antitrust liability for information sharing related to critical infrastructure protection). See also: National Cooperative Research Act, Pub. L. No. 98-462, 98 Stat. 1815 (1984) (expressly limiting antitrust liability for research joint ventures).
127. Suchman (2013).
128. Liu et al. (2013).
129. H.R. 624, 113th Cong. (1st Sess. 2013).
130. Suchman (2013).
131. The three agencies recently submitted their reports to the president. See: Daniel, Michael (2013) *Incentives to Support Adoption of the Cybersecurity Framework*, August 6. Available at: http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.
132. Rashid, Fahmida (2013) "Report Shows 'Uneven Progress' in Cybersecurity Information Sharing," *SecurityWeek*, May 30. Available at: http://www.securityweek.com/report-shows-uneven-progress-cybersecurity-information-sharing.
133. Congress has noted in the past that the security-clearance process is very difficult to navigate, even for federal government employees. See: *Security Clearance Reform: Moving Forward on Modernization: Hearing Before the Oversight of Government Management, the Federal Workforce, and the District of Columbia Subcomm. of the S. Comm. On Homeland Sec. and Gov't Affairs*, 111th Cong. (2009). Available at: http://www.gpo.gov/fdsys/pkg/CHRG-111shrg53837/pdf/CHRG-111shrg53837.pdf.
134. Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf.
135. H.R. 5026, 111th Cong. (2nd Sess. 2010).
136. S. 1353, 113th Cong. (1st Sess. 2013).
137. See: "STIX. Structured Threat Information eXpression." Available at: http://stix.mitre.org/.
138. See: "Trusted Automated eXchange of Indicator Information." Available at: http://taxii.mitre.org/.
139. North American Electric Reliability Corporation (2012) *Severe Impact Resilience: Considerations and Recommendations*. May 9. Available at: http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf. See also: NERC and DOE (2010) *High-Impact, Low-Event Risk to the North American Bulk Power System*, June. Available at: http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.
140. An "island" is load where power flow from the utility has been disconnected but which continues to be powered by one or more distributed generators.
141. See, for example: Tweed, Katherine (2013) "3 Ways Superstorm Sandy Could Change Utilities Forever," *GreenTechGrid*, October 29.
142. U.S. Department of Homeland Security (2013) *National Response Framework: Second Edition*, May (National Response Framework). Available at: http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.
143. U.S. Department of Homeland Security (2010) *National Cyber Incident Response Plan. Interim Version*, (Interim NCIRP) September. Available at: http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.
144. National Response Framework.
145. *Ibid*, pp. 3-4, 30-33.
146. *National Response Framework*, pp. 31-6, and U.S. Department of Homeland Security (2011) *National Preparedness Goal* (first edition), September. Available at: http://www.fema.gov/pdf/prepared/npg.pdf.
147. National Response Framework, pp. 31-8.
148. The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 USC. 5121 et seq.
149. Federal Emergency Management Agency, *Hurricane Sandy: Timeline*. Available at: http://www.fema.gov/hurricane-sandy-timeline.
150. U.S. Department of Housing and Urban Development (2013) *Hurricane Sandy Rebuilding Strategy*, Hurricane Sandy Rebuilding Taskforce, August. Available at: http://www.whitehouse.gov/blog/2013/08/19/hurricane-sandy-rebuilding-strategy-helping-communities-prepare-impacts-changing-cli.
151. U.S. Department of Housing and Urban Development (2013) *Hurricane Sandy Rebuilding Strategy*, Hurricane Sandy Rebuilding Taskforce, August. Available at: http://www.whitehouse.gov/blog/2013/08/19/hurricane-sandy-rebuilding-strategy-helping-communities-prepare-impacts-changing-cli. Edison Electric Institute (2013) "Before and After the Storm: A Compilation of Recent Studies, Programs, and policies related to Storm Hardening and Resiliency," *EEI*. Available at: http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/Before%20and%20After%20the%20Storm.pdf.
152. Interim NCIRP, p. 1.
153. For more information, see: Federal Emergency Management Agency (2012) *National Level Exercise (NLE) 2012*. Available at: http://www.fema.gov/national-level-exercise.
154. Federal Emergency Management Agency (2013) *National Level Exercise 2012: Quick Look Report*, March. Available at: https://www.llis.dhs.gov/sites/default/files/National%20Level%20Exercise%202012%20Quick%20Look%20Report.pdf.
155. See Serbu (2013).
156. National Response Framework, pp. i, 7
157. Interim NCIRP, p. v.
158. National Response Framework, pp. 31-7.

159. Interim NCIRP, pp. 20-24.
160. National Response Framework, p. 13.
161. Interim NCIRP, pp. K1-11.
162. National Response Framework, p. i.
163. National Response Framework, p. 13.
164. National Governors Association (2013) *Act and Adjust: a Call to Action for Governors*, September, pp. 2-3. Available at: http://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-hsps-publications/col2-content/main-content-list/act-and-adjust-a-call-to-action.html.
165. English, Charlie (2013) "Cyber Incident Response: Bridging the Gap Between Cybersecruity and Emergency Management," Statement for the Record on behalf of the National Emergency management Association, Hearing, House Homeland Security Committee, Subcommittee on Emergency Preparedness, Response, and Communications, October 30, pp. 5-6.
166. St. John, Jeff (2013) "Report: U.S. Smart Grid Cybersecurity Spending to Reach $7.25 Billion by 2020," *Greentech Grid*, April 17. Available at: http://www.greentechmedia.com/articles/read/report-United States-smart-grid-cybersecurity-spending-to-reach-7.25b-by-2020.
167. Malkin, David, and Paul Centolella (2013) *Results-Based Regulation: A Modern Approach to Modernize the Grid*. Available at: http://www.analysisgroup.com/uploadedFiles/Publishing/Articles/Centolella_GE_Whitepaper_Electricity_Regulation.pdf.
168. Keogh and Cody (2013).
169. DOE estimated costs of $6 billion, a figure that is near the $6.4 billion mid-range estimate prepared by Anderson Economic Group. For a summary of estimates of the blackout's costs, see: Electric Consumers Resource Council (2004) *The Economic Impacts of the August 2003 Blackout*, February 9.
170. U.S.-Canada Power System Outage Task Force (2004) *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, August, p. 131. While the information system failures in this case were not the result of a malicious attack, the Task Force nonetheless found, "potential opportunities for cyber system compromise of Energy Management Systems (EMS) and their supporting information technology (IT) infrastructure," and supported new cyber and physical security standards.
171. See, for example: *Sunoco Inc. v. Kimberley Clark Pennsylvania, LLC. et al.*, Civil Action No.: 213-cv-01822, U.S. District Court for the Eastern District of Pennsylvania. While not a cyber incident, in this case, the failure of electricians at a Pennsylvania paper mill to follow procedures allegedly led to a multimillion-dollar refinery outage.
172. Note that similar assessments are an element of the National Infrastructure Protection Program. See: U.S. Department of Homeland Security (2009) *National Infrastructure Protection Plan*. Available at: https://www.dhs.gov/sites/default/files/publications/NIPP_Plan.pdf. And, for the energy sector-specific plan, see: U.S. Department of Homeland Security and U.S. Department of Energy (2010) *Energy Sector-Specific Plan*. An Annex to the National Infrastructure Protection Plan. Available at: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG