TRUMAN CENTER

Keeping the Lights On

The Critical Role of U.S. States in Electrical Sector Cybersecurity

Andreas Mueller
Peter Liebert
Austin Heyworth

April 2017

PREFACE

Protecting the U.S. electrical grid from cyberattack is particularly important—it is the lynchpin for all critical infrastructure sectors. However, security vulnerabilities in the electrical sector have too often focused on the federally-regulated Bulk Electric System. This has come at the expense of the less visible but more widespread non-Bulk Electric System, which is usually regulated at the state level. This paper takes an in-depth look at the non-Bulk Electric System, illustrating its cybersecurity issues and scrutinizing its regulators. For the non-Bulk Electric System to reach an acceptable level of cybersecurity, as well as to help achieve resiliency across the entire U.S. grid, states can and should lead the way—starting by implementing these recommendations. The time is now.

The opinions expressed in this document are of the authors' alone and do not reflect the opinions or positions of any outside institution.

TABLE OF CONTENTS

ABOUT THE AUTHORS

Andreas S. Mueller

Andreas S. Mueller is Chief of Federal Policy for the California Military Department, where he handles national security policy in the Governor's Washington D.C. office, and serves as Executive Director of the Governor's Military Council, California's statutory advisory body to the Governor and State Legislature on national security and defense policy. Mueller is also a Partner at the Truman National Security Project, a Washington D.C. think tank, where he previously served as Co-Chairman of its Cybersecurity Expert Group. In his eleven years in D.C. he previously served as Legislative Director to Congressman Glenn Nye of Virginia, Senior Legislative Assistant and Military Legislative Assistant to Congressmen Jerry McNerney of California, Deputy Finance Director for Jerry McNerney's political campaign, as well as Assistant Campaign Coordinator for then Rep. Lynn Woolsey. Mueller is a California native and has called D.C. his home since 2006. He received his B.A. in Philosophy from the University of California, Santa Barbara, and his Masters of Public Policy, Management at Georgetown University.

Peter Liebert

Peter Liebert was appointed as Chief Information Security Officer and Director of the Office of Information Security at the California Department of Technology in 2016. Liebert had been senior product manager at FireEye Inc., where he was previously a threat assessment manager. He served in several positions at the United States Cyber Command, including special assistant in the Office of the Secretary of Defense for cyber policy and senior cyber policy analyst. Liebert served as cybersecurity and logistics analyst in the Office of the Chief of Naval Operations and was lead for the Palestinian Logistics Mentoring and Warehouse Information Technology Program at DynCorp International. He served as an officer in the U.S. Navy for eight years. He earned a Master of Public Administration degree from the Harvard University, Kennedy School of Government and a Master of Science degree in international security from Cranfield University.

Austin Heyworth

Austin Heyworth is Public Affairs Manager for Uber Technologies in California, where he represents the ridesharing giant on state government issues. He is a former college quarterback who transferred that competitiveness into a career in politics. Most recently, he served on the staff of California Assemblywoman Jacqui Irwin and previously worked for Assembly Speaker John A. Perez. His policy work has focused on the issues of higher education, technology and privacy, emergency services, and cybersecurity. He was the primary staffer for the Chair of the Veterans Affairs Committee. He has also built experience running state-level political campaigns, as well as Speaker Perez's statewide

campaign for Controller. His career goal is to continue to bridge the gap between the tech industry and government and to work on policy that will modernize the public's view of cybersecurity.

The authors would like to acknowledge contributions and assistance from Mike Breen, Leigh O'Neill, Dan Paltiel, Matthew Rhoades, Caitlin Howarth, Brandon Fureigh, Graham West, Welton Chang, Michael McNerney, and many unnamed government employees interviewed for this project.

INTRODUCTION

Malicious actors in cyberspace are actively seeking to exploit vulnerabilities in domestic computer networks to harm U.S. national and economic security. By interrupting the availability, integrity, and confidentiality of information networks, cyberattacks threaten critical infrastructure, which could have a debilitating effect on the economic, health or national security of Americans. In particular, the risk to the electrical sector is highly concerning.

The electrical sector is the lynchpin for all other critical infrastructure sectors, from financial systems to the water supply. Without power, none of these sectors can function. The electrical grid, for this reason, can be seen as the single point of failure to the American way of life, and cyber breaches in this critical sector are on the rise year after year (Trend Micro & OAS 2014, 6). In fact, the FBI recently declared cyberattacks on this sector more potentially dangerous than terrorism (McGuinness 2014; Miller 2013). According to FBI Director James Comey, "Virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates and terrorists" (Comey 2016).

The distinct lack of cybersecurity protection for the U.S. electrical grid has been of concern for over a decade. After President Clinton identified electrical grid cybersecurity as a threat in 1996 via Executive Order 13010 and Presidential Decision Directive 63, each of his successors has cited it as a major challenge. There have been dozens of official government and independent reports analyzing the issue, attempting to provide remedial recommendations to begin to mitigate this critical threat to our way of life.

These reports, however, tell an incomplete story. Often overlooked is that most analyses of this issue have only covered a portion of the electrical grid—specifically, the Bulk Electric System (BES). This is not by happenstance. The BES is the backbone of the country's electric grid and is the most easily understood portion of the electric system, consisting of big power plants and long-stretching power lines that generate and transmit electricity. Accordingly, a common popular imagining of a cyberattack on the electrical grid tends to involve a nuclear reactor, a BES electricity generation component, exploding with Hollywood-style drama.

Cyber resiliency in the electrical sector is not only a BES issue, though. The less-examined portion of the electrical grid is named "the non-Bulk Electric System," or non-BES. The concept of the non-BES is as simple as its name. The BES is like the brain, heart and major arteries of the electric grid; it is critical in that it governs and supplies blood to the rest of the body. In contrast, the non-BES system is the nervous system, limbs, small veins, and other organs—greater in number and just as critical when taken as a whole.

Yet many do not consider the non-BES of equal weight when thinking about U.S. national security. Indeed, on its surface, the non-BES might appear to have little significance or national importance. This assumption changes dramatically, however, when put in context. The electrons feeding the local DMV, a 911 call center, and a U.S. military base are all part of the non-BES. Unfortunately, out of the spotlight, the non-BES has failed to garner the attention of regulators to enforce even basic cybersecurity standards like those in the BES (Campbell 2015).

However, when the power goes out as a result of a cyberattack, victims are likely to call their power company, city officials, and state officials—not the Department of Homeland Security. The Non-BES, including power companies' electrical distribution infrastructure, is overseen by a patchwork of mostly state regulatory entities whose personnel are generally less proficient when it comes to cybersecurity than their federal BES regulator counterparts (Campbell 2015). As journalist Ted Koppel writes, "American democracy rests on a foundation of competing tensions among local, state, and federal laws, and laws governing the electric power industry reflect those tensions" (Koppel 2015). Even so, a lot of the problems plaguing national-level BES do not overlap with the non-BES sector; they are unique and therefore require unique solutions.

U.S. states are responsible for overseeing most of the electrical grid. However, many are neglectful in formulating statewide cybersecurity policies and funding cybersecurity capabilities of consequence (Campbell 2015; Goure 2016). This is concerning, given the large swath of responsibility and limited engagement of this group. U.S. states have a clear leadership opportunity to improve the cybersecurity of the electrical sector. Doing so would improve the overall resilience of the electrical grid and allow states to maintain control of their varied and critically important electrical power networks, forgoing probable blanket federal regulatory actions and helping to focus the federal government on preventing and reacting to catastrophic and high-risk attacks on the nation.

This paper takes an in-depth look at the non-BES, analyzes its cybersecurity issues, and scrutinizes the regulators in charge—where they exist, where they do not, and who they should be—to provide actionable recommendations that should elevate the non-BES to an acceptable level of cybersecurity. Each of the recommendations also addresses cyber resiliency to ensure energy reliability before, during, and after a cyber incident in order to best capture the entire scope of the cyber threat.

While this paper is not a comprehensive, standalone document that attempts to address all aspects of cybersecurity issues with the non-BES, its recommendations aim to help states along the path of developing a truly robust cybersecurity resiliency program. America must strive towards a comprehensive cybersecurity solution that is inclusive of the private, local, federal, and state governments; this paper can serve as the first piece of that goal.

States should endeavor to implement these recommendations to help harden against a potentially catastrophic cyber event. Currently, the lack of information and understanding, scarce funding, and unwittingly misplaced priorities by senior leaders have meant that appropriate action on non-BES has not been taken. We sincerely hope that this paper can help in some way to change this pattern of behavior, and, in layman's terms, help "keep the lights on."

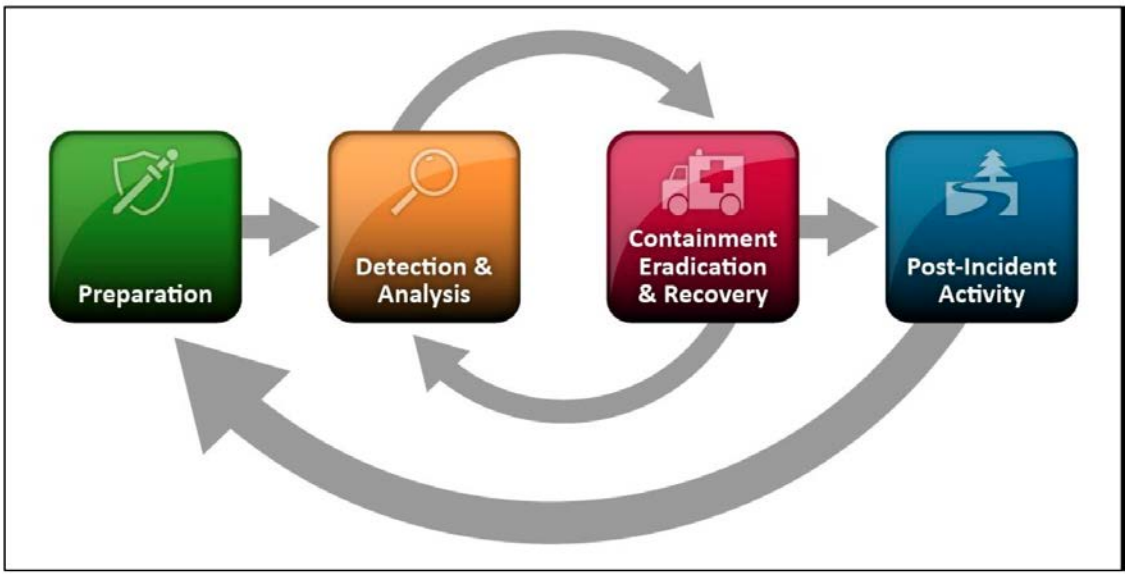


Figure 1 Incident Response Lifecycle (Source: NIST Special Publication 800-61)

The 22 actionable recommendations to follow are spread across six principle policy areas where gaps in current cybersecurity policy exist: state government cybersecurity, cybersecurity information sharing, private sector and state cooperation, establishing standards, cybersecurity education and workforce development, and incident response. These are the six primary strategic areas of cybersecurity policy, are clearly influenced by U.S. states, and have the most significant requirements for improvement. These recommendations are based on original research through interviews and discussions with cybersecurity and electrical industry experts, surveys of current state and federal cybersecurity practices and policies, and existing literature containing critical analysis of electrical sector cybersecurity. They are as follows.

TABLE OF RECOMMENDATIONS

State Government Cybersecurity

1. Governors should designate a Cybersecurity Coordinator or elevate their state CISO to act in this capacity.
2. Each state Cybersecurity Coordinator should have a direct line of communication and interact regularly with the federal Cybersecurity Coordinator to plan and strategize for cyber incidents that threaten national security, as well as share best practices.
3. To protect PUCs during audits and collection of information, necessary legal protections should be afforded for handling and storing critical infrastructure and cybersecurity information, such as that which includes personally identifiable and proprietary information, and should restrict public disclosure requests, as is done in several states.

Cybersecurity Information Sharing

4. Establish and empower a State Integration Center or Information Sharing Hub.
5. Encourage information sharing through existing platforms such as fusion centers and the MS-ISAC.
6. Information quality.

Private Sector and State Cooperation

7. Commit to Forming Public-Private Collaboration and Labor Exchanges
8. Promote hunting for network compromises as well as response activities.

Establishing Standards

9. States should require NERC CIP baseline standards.
10. States should take advantage of tools the Department of Energy offers to mitigate the lack of cybersecurity expertise of PUC personnel.
11. To verify the adoption of CIP standards, states should empower PUCs to hire expert staff and perform on-site audits and reasonable penetration testing of non-BES stakeholders, publicly releasing their CIP compliance.
12. Funding and revenue incentives

Cybersecurity Education and Workforce Development

13. Promote cybersecurity education early.
14. Require cybersecurity in the classroom
15. Ensure electrical sector regulators have cybersecurity expertise.
16. Governors should lead the nation in cybersecurity education and workforce development.
17. Governors should be a catalyst for cutting-edge cybersecurity research.
18. Work to get more women in high tech and cybersecurity fields.

Incident Response

19. Governors should lead the way in domestic cybersecurity response, allowing the federal electrical sector regulators to focus more on advanced threats.

20. States and governors should be directly involved in national cyber incident response efforts and policy making.
21. Governors should take further advantage of DHS cyber programs.
22. The National Guard should be fully resourced, equally trained, equipped and authorized to use all available tactics, and made a key part of domestic cyber incident response.

II. CURRENT THREAT LANDSCAPE IN THE NON-BULK ELECTRIC SYSTEM

The U.S. electrical power system is split between two broad categories: namely the Bulk Electric System (BES) and the non-Bulk Electric System (non-BES) (see figure 2). The BES includes electrical generation and transmission elements of 100 kV or higher, with few exceptions, and does not include local distribution of electricity (NERC 2015). The BES is overseen by federal entities, while the non-BES is primarily under the purview of states but can also be governed by municipalities (Campbell 2015). Once electricity is in the non-BES for distribution to the consumer, "no federal regulations apply" (Koppel 2015, 32). The non-BES system is actually the larger of the two, representing approximately 80 percent (Campbell 2015, 13) of the electrical grid (Peter Behr and Blake Sobczak 2015), as it consists primarily of elements involved in the distribution of electricity to the consumer rather than generation or high-voltage transmission (Bogorad and Nurani 2012).

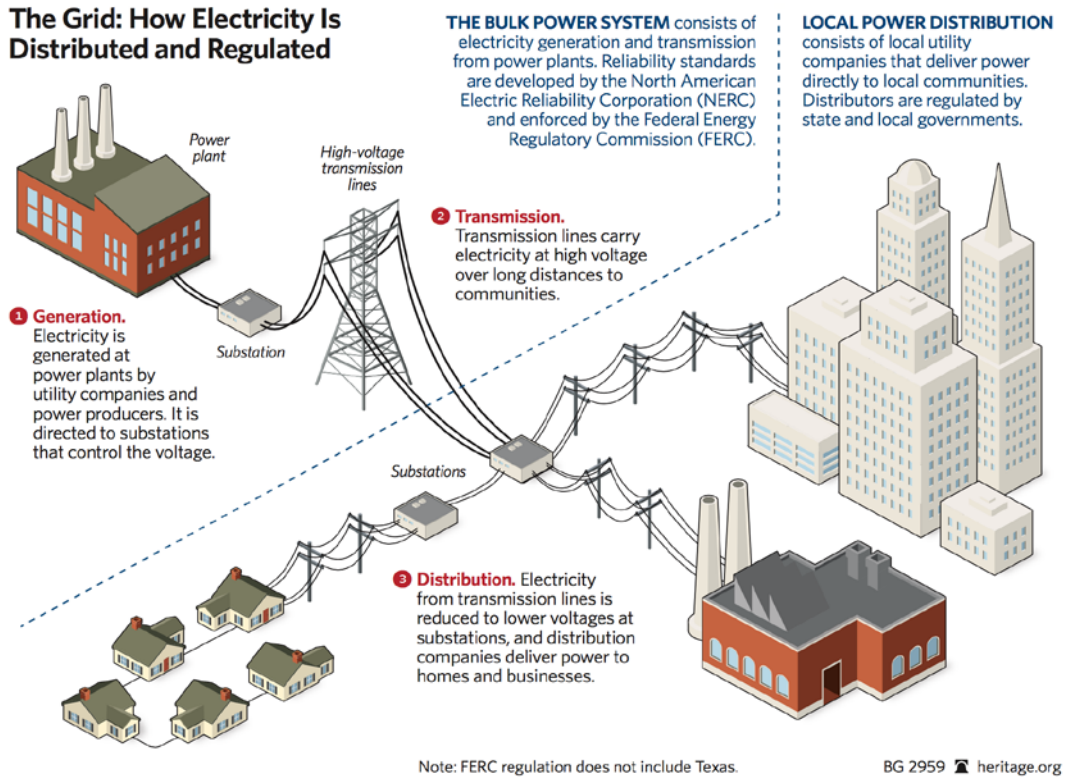


Figure 2 The Grid: How Electricity is Distributed and Regulated (Source: Jonathan Lesser, 2014)

The BES, under the regulation and purview of NERC, must adhere to baseline cybersecurity standards. While these standards have been continually improved over the last half decade, there is still some controversy on how effective this approach has been. However, non-BES stakeholders operate outside of federal regulations and lack even minimum mandatory cybersecurity standards because the non-BES is legally outside of

federal jurisdiction (NERC 2015). The crux of this entire issue is that electricity delivered to consumers is not covered by federal security regulations, as per the preference of industry (Koppel 2015). Yet the failure of non-BES could be significant, particularly for systems supporting critical sectors of the economy. These systems distribute electricity directly to all other critical infrastructure industrial sectors, including water and oil pipelines, telecommunications, and government operations. While the definition of BES was made to be more inclusive in 2014, the non-BES still remains a critical aspect of the power grid and is simultaneously the least regulated.

IMPORTANCE OF NON-BES SECURITY

A cyberattack on the non-BES distribution system could have serious national consequences. Past distribution system failures have cascaded, proliferating to the electrical grid's BES backbone (Campbell 2015). Subsequently, this effect could be multiplied in the face of several distribution system failures. For example, federal regulators found that one of the causes of the 2011 Southwest Blackout—in which cascading outages caused 2.7 million customers to lose power at an estimated cost of $100 million to consumers (National University System Institute for Policy Research)—was the failure of the Imperial Irrigation District's non-BES distribution system (FERC and NERC 2012; Bogorad and Nurani 2012).[1] This risk only increases as new technology is introduced to the non-BES.

To illustrate this further, U.S. military facilities are almost wholly reliant on the public electrical grid and utilities, and are therefore served by the non-BES (GAO 2015). The security implications of cutting off electricity to a military base should be apparent since it may be easier to affect base operations this way than via direct cyberattack on military networks, a reality echoed by the Department of Defense (DOD) in 2014. In a GAO report, DOD asserted that cyberattacks on installation electrical systems could have serious effects, including the destruction of critical infrastructure, which could degrade or compromise DOD's ability to conduct its missions (GAO 2015, 20,36,44). This was further reinforced by a former top-ranking National Security Agency (NSA) technology professional, who remarked that while the agency itself is protected, "the electric power coming into the agency is not" (Koppel 2015, 32).

Non-BES distribution systems are incorporating more and more smart infrastructure aimed at optimizing the real-time, automated physical operation of electrical appliances, many of which are vulnerable to cyberattack (Michael Hayden, Curt Hébert, and Susan

[1] After the incident, FERC and NERC directed regional BES entities to evaluate their networks for non-BES systems that could affect the BES. In 2012 the Western Electricity Coordinating Council asserted that it was doing so (WECC 2012, 3). However, the example highlights the possibility of the non-BES affecting the BES, which could in turn happen again. For example, what if the WECC, who self certifies that it meets NERC standards, fails to account for a different or growing sub-100kv non-BES system that could affect the BES, or a non-BES in a different U.S. region? What if it was more than 1 but 2, 10, or 100 non-BES networks that are simultaneously disrupted by an advanced cyberattack? In addition, and perhaps most important, the definition of the BES in federal law 16 U.S.C. § 824o(a)(1) does not include any elements "used in the local distribution of electricity."

Tierney 2014). These include: off-the-shelf software, advanced metering, advanced customer management systems, distribution automation, two-way electrical flow technologies (including the ability for utilities to communicate with and control major electrical devices such as heating and air conditioning), and other smart grid infrastructure (Campbell 2015). Moreover, some of these technologies currently communicate over vulnerable media, such as Wi-Fi and unencrypted radio waves, compounding the negligence of companies who do not bother to update or change default passwords on Industrial Control Systems (ICS) and supervisory control and data acquisition (SCADA) systems (ICS-CERT 2016; Longstaff 2015).

Further, renewable energy and two-way electrical flows within the non-BES will blur its technical definition, making differentiating between it and the BES systems more difficult. This may create jurisdictional issues between states and federal regulators, thereby increasing the risk the non-BES poses to the BES (Michael Hayden, Curt Hébert, and Susan Tierney 2014). The future growth of a smart grid is a central focus of electrical sector cybersecurity concerns; however, unlike the BES, much of the non-BES has not yet been made smart. It is estimated that utility companies will spend $7 billion on cybersecurity upgrades by 2020, but it has not been made clear what fraction of that will go to protect non-BES systems (Michael Hayden, Curt Hébert, and Susan Tierney 2014). Ultimately, as this new technology propagates to the non-BES, its risk to the BES will increase (NERC 2015).

ELECTRICAL GRID VULNERABILITIES

Efforts to address this critical vulnerability exist, but the computer backbones that critical infrastructure utilizes to operate, known as industrial control systems (ICS), are still susceptible. In 2015, the Department of Homeland Security (DHS), for example, responded to 295 known cyber incidents that impacted critical infrastructure, 46 of which were in the energy sector, the second most targeted category (ICS-CERT 12-15). The actual unreported numbers are likely an order of magnitude higher. [2]

This is particularly concerning as cyber intrusions into ICSs can allow a malicious actor to manipulate this weakness and cause catastrophic failure (ICS-CERT 2015). There is little data inside an ICS that could be easily leveraged for monetary gain, such as credit card data or personal information, so there is little reason for threat actors to target these systems unless they have a larger nefarious goal in mind or a desire to hold the asset at risk for ransom (a risky endeavor). In other words, these actors are not likely to steal anything; rather, they are there to find out how to undermine the system itself (ICS-CERT 12-15). The defense and intelligence communities call this

[2] Unfortunately, the aforementioned numbers use cases that were self-reported by the power companies themselves, leading prominent researchers to assert that they may drastically underestimate the scope of this problem as they continue to find a large number of ICSs inadequately secured through open and closed source analysis and research (David Kruger 2012, 1).

"intelligence preparation of the battlespace," (ICS-CERT 12-15) and it is often a harbinger of a potentially devastating attack.

With evidence pointing to vast vulnerabilities in the U.S. electrical power ICS, state governments must take the threat of cyberattack seriously and ensure that all available measures to protect these critical systems are taken. In December 2015, a cyberattack on the Ukrainian power grid disrupted power to hundreds of thousands of people (Goure 2016). The network (IP) addresses linked to critical infrastructure are actually available online, increasing their vulnerability (Shodan 2017). And in California, a data breach report by the attorney general detailed the security failures of government agencies and businesses in exposing 50 million personal records, from 2012 to 2015.

To achieve this goal, states must address the problem of electrical grid vulnerabilities using the same methodology that computer security incident responders use and broadly address the issue before, during, and after an incident (see figure 1). Whereas electrical companies' response methodology focuses on their individual needs, states must take a strategic approach and act in a manner that can positively influence the plans that companies are developing.

III. STATE LED OPPORTUNITIES IN NON-BES SECURITY

As varied as the stakeholders are in the non-BES space, there are common issues that states are in a leading position to affect. However, government oversight of the electrical sector is spread across a scattered regulatory structure, presenting a challenge for decision makers seeking to deliver effective cybersecurity across the entire system. The following section provides recommendations and showcases best practices across six areas in an effort to improve cybersecurity across state government: State government cybersecurity, private sector and state cooperation, information sharing, standards, education and workforce, and incident response. It is important to note that many of these recommendations apply to not only the electrical sector but to state cybersecurity in general.

STATE GOVERNMENT CYBERSECURITY

Electrical sector stakeholders (utilities and other entities operating in the non-bulk electrical system, hereafter referred to as non-BES stakeholders) at the state government level face the same challenge as the federal government in providing cybersecurity protection for vital infrastructure. This is a problematic gap in electrical grid security as state governments could potentially have a larger effect on electrical sector cybersecurity as they regulate the larger non-BES where cybersecurity regulation is virtually absent, can enact policies faster than the federal government and Congress, can better customize resources to the area, and are closer in proximity if onsite assistance is imperative.

Unfortunately, states have invested little in critical infrastructure protection, including in the electrical sector. Indeed, state Chief Information Officers often indicate that the lack of adequate funding is a major barrier to effective cybersecurity (NASCIO & Deloitte 2012) and that state and local governments typically spend less than five percent of their IT budget on cybersecurity (Lipman 2015). This is troubling, especially considering the high-profile, successful attacks on federal government networks, such as the June 2015 breach at the Office for Personnel Management, which invested heavily in cybersecurity. As one prominent cyber expert put it, "if the federal government is considered the class valedictorian of security, states are barely graduating" (Kevin Mandia 2015).

FUNDING

According to a 2014 Deloitte report for the National Association of State Chief Information Officers (NASCIO), roughly half of states spend between 1-2 percent of overall IT budgets on security—a number significantly below private sector averages. Further, 45 percent of states lack an approved strategy for long-term security budgeting. While state budgets for cybersecurity are increasing slightly, current funding levels are not adequate to support information sharing infrastructure and qualified personnel necessary to provide ongoing security benefits.

State budgets for cybersecurity are inadequate and lag behind the private sector considerably. Current funding needs to be increased and substantiated by a process that matches funding to identified risks or weaknesses in cybersecurity operations. Most states have not separated out cybersecurity as a distinct category of an overall IT budget, resulting in inadequate funding and operational attention. This is an unsustainable approach. Most networks overseen by state regulators, to include the electrical sector, may be highly vulnerable.

STAKEHOLDERS

Unlike the federal government, key state stakeholders are not nearly as well-known, even among energy and cybersecurity professionals. Governors lead a disjointed incident response and oversight effort, overseeing several critical entities, including state public utility commissions[3], emergency services agencies, energy officials, chief information and security officers (CIOs and CISOs), law enforcement and the National Guard. This oversight structure is further fragmented across 50 different jurisdictions, each with different laws and regulations – to put it bluntly, there are a large number of stakeholders in the non-BES space and each has its own capabilities, concerns, and priorities. To understand the varied stakeholders at play is to understand a critical component of why the non-BES electrical grid cybersecurity has so far been largely ignored. Below is a review of the primary non-BES stakeholders:

[3] Some states have Public Service Commissions (PSCs). While there are some differences, this report chooses to refer to both as PUCs for simplicity sake, as the recommendations made for PUCs can be also made to PSCs.

State Public Utility Commissions

States oversee the non-BES via public utility commissions (PUCs), which are tasked with ensuring system reliability. PUCs primarily oversee monopoly-empowered private utility companies,[4] which serve 70 percent of all electrical power customers nationwide.[5] One important aspect of PUCs is that they regulate the retail price of electricity and the ability of utilities to pass infrastructure investment costs on to the consumer (i.e. return on equity), including those resulting from strengthening cyber defenses. This authority means PUCs wield a powerful incentive-based tool for cybersecurity investment. Unfortunately, while state PUCs administer strong electrical reliability measures, evidence shows that they have done little to implement cybersecurity provisions or incentivize investment (Peter Behr and Blake Sobczak 2015; PUC Official 2-16 & 1-17; Koppel 2015, 31; Michael Hayden, Curt Hébert, and Susan Tierney 2014, 34).[6] PUCs are also represented nationally by the National Association of Regulatory Utility Commissioners (NARUC) which serves as major forum for ensuring State Public Service Commissioners provide reliable utility service at fair, just, and reasonable rates (NARUC 2017).

Governors

Governors have a principal leadership role in directing all aspects of electrical sector cybersecurity including, but not limited to, information sharing, workforce and education, standardization, and incident response (Peter Behr and Blake Sobczak 2015). As the head of all state agencies, including the almost wholly federally funded National Guard, governors are ultimately responsible for all non-federal response efforts and leveraging federal resources to address state-level critical events.

State Chief Information Officer (CIO)

CIOs direct state resources to procure information technology (IT) and set IT requirements or recommendations for the entire enterprise of state government. One of the starkest contrasts among state agency cybersecurity responsibility is the authority of state CIOs. Only a little over half of state CIOs have the authority to impose requirements on executive agencies, and only 14 percent have that authority over all state government (NASCIO & Deloitte 2012). This means it is not uncommon for states like California, for instance, to have multiple CIOs across various agencies, each employing different cybersecurity standards and practices that do not match those recommended by the state CIO. This kind of decentralized strategy without baseline standards is highly risky to an interconnected enterprise; hackers can take advantage of the weakest links in state

[4] Specifically, PUCs oversee investor-owned utilities (IOUs), which are utilities that are privately owned. They are rate regulated and authorized to achieve an allowed rate of return. 265 IOUs provide electricity for 70 percent of the U.S.(FERC 2017; McDonald 2012).

[5] Federal, municipal utilities, rural cooperatives and independent power producers service the other 30 percent of the U.S. population. In some cases, rural cooperatives and municipal utilities are also overseen by PUCs, but most are controlled by utility boards or local governments (DOE 2012).

[6] There are a handful of states whose PUC is at least beginning to implement cybersecurity requirements. This report cites an example of one of the most advanced in the PUC recommendation later in the paper.

networks by using use those entry points to exploit states in their entirety (Raduege 2013). States' unwillingness to standardize cybersecurity requirements for their own networks may proliferate similar risk into the entities they oversee, such as the interconnected electrical sector. The importance of standardization is a key topic of this paper.

State Chief Information Security Officer (CISO)

State CISOs are responsible for ensuring the confidentiality, availability, and integrity of state systems. While the role of CISO varies from state to state, it is typically charged with the development and oversight of the state's cybersecurity baseline standards. In addition, multiple states (e.g. Washington) have the CISO chair or lead the state's centralized cybersecurity operations center. The CISO has traditionally reported to the state CIO; however, as cybersecurity has become increasingly important over the last few years, some states have taken a page from private industry's best practice by elevating the CISO role to the equivalent of the state CIO.

State Emergency Management Offices

State emergency management offices are the statewide lead agency for emergency planning, information sharing, response operations, as well as communication to federal agencies for major cyber incidents that threaten the state, its people, and its critical infrastructure.[7] The DHS is the federal lead for these efforts and works with state emergency managers to this end; however, this relationship is occasionally tenuous on account of conflicting priorities, as evidenced by past incidents such as Hurricane Katrina in 2006 (GAO 2016). This puts emergency management officials at the forefront for cybersecurity incident response. Several emergency mangers, such as those from Washington and Georgia, are also dual-hatted as the state National Guard Adjutant General (DoD 2014). Law enforcement also has a role here: State police are often responsible for the collection of evidence and prosecution of criminal events, including those in cyberspace.

State Energy Officials

Each governor has a designated energy official who advises both them and state legislators on energy policy.[8] These State Energy Officials have a whole of state government perspective across public and private stakeholders, engaging on a litany of policy issues such as research and development, private sector partnerships, environmental quality, domestic energy development, energy efficiency, emergency response and mitigation, and state energy fund allocation. These funds include some federal funds for alternative, renewable, and energy efficiencies for a select number of states via the U.S. State Energy Program. Energy officials are important policy figures, as

[7] The structure of emergency services offices varies widely among states; this summary represents a generalization.

[8] Roughly half of all energy officials are also the governor's direct energy policy advisor, although some are contained within state PUCs.

they have the authority to mandate and guide state-level research, demonstrate and implement emerging energy technologies, and communicate all state energy needs at the executive level. One key element to their work are the state Energy Assurance Plans (EAP), which help states design a blueprint to assure reliable and resilient energy infrastructure. However, research shows that energy officials are not heavily involved in cybersecurity activities, despite each receiving at least some federal funding (NASEO 2015). Another important factor is that state energy officials are represented federally by a national association called the National Association of State Energy Officials (NASEO), the forum for collaborative policy decision-making and sharing of best practices.

National Guard

The National Guard currently possesses much of states' cyber incident response capability, a result of a lack of state focus on cybersecurity, federal policy, and subsidized federal funding. Their dual mission responsibility for domestic response and wartime offers governors highly proficient military-grade cybersecurity capabilities at little cost to the state, as the National Guard is almost wholly federally resourced. As described below, states are beginning to take advantage of this key resource, yet a lack of support from the DOD has constrained their use.

The Federal Government

States are autonomously responsible for non-BES cybersecurity and are afforded little support by the federal government. DHS and the Department of Energy (DOE) (DOE 2014; DHS 2015) provide ad hoc financial resources, such as grants; absent a presidential emergency declaration, however, "the government's role in [state] effort[s] is to share information and encourage enhanced security and resilience" (Stempfly 2013; DHS 2013b).[9] The DOE does not have a cybersecurity regulatory responsibility, which coincides with the fact that there is not a federal agency that has been tasked with the responsibility of defending states or providing states access to significant cyber defense capability.[10] Further, "[states], in coordination with energy asset owners and operators, have primary responsibility for prioritizing the reestablishment of critical infrastructure" (DOE 2013). This is important because state governments do not possess the same personnel skillsets, technology resources, and adequately defined and delineated roles and responsibilities as their federal counterparts. This has led cybersecurity experts to deem state information systems as "porous" and having "the weakest [cybersecurity] infrastructure," (Raduege 2013, 2009) when compared to the federal government. This is echoed by officials at the National Governor's Association (NGA) who have said, "nobody [in the federal government] is looking out for states" (NGA 2013).

[9] This is echoed by officials at the National Governor's Association (NGA) who assert, "nobody [in the federal government] is looking out for states" (NGA personal communication 2013).

[10] The president possesses broad powers, and the ability to expand those powers, during emergencies (Fleming and Goldstein 2011). However, repeated presidential declarations for domestic cyber events would likely not be a long-term solution to state cybersecurity (see further discussion in the Incident Response section of this report).

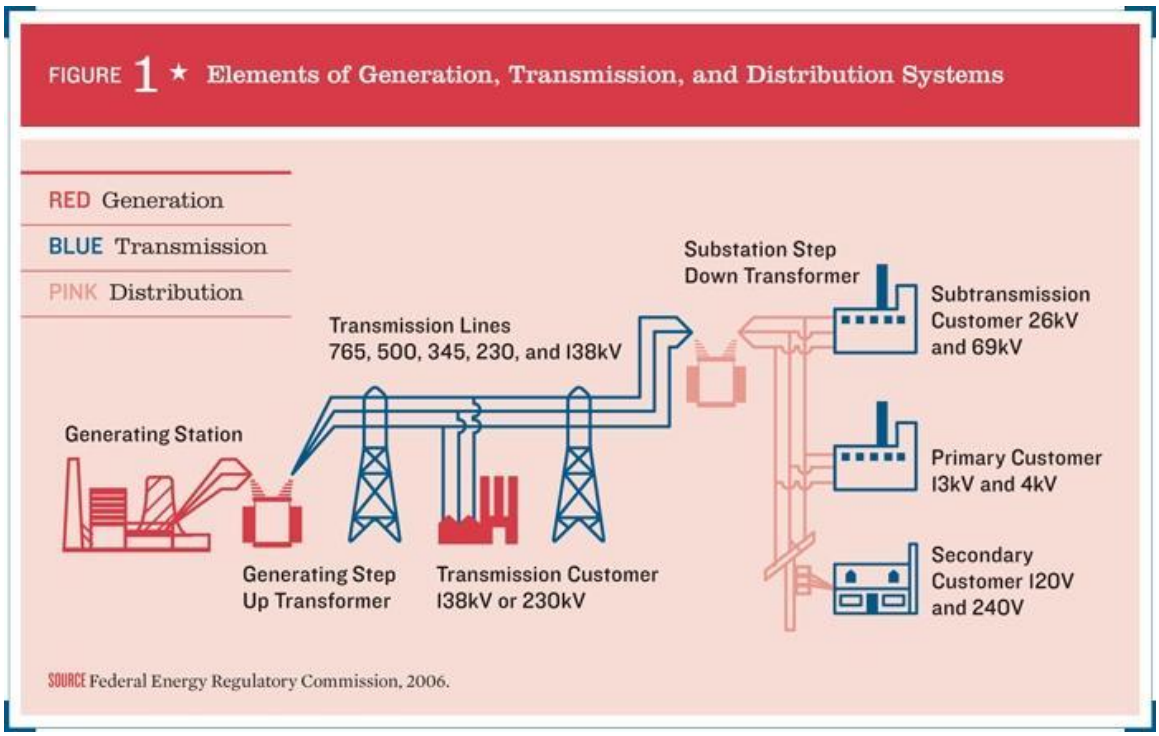
Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) is a five-member, bipartisan, independent agency that, among other activities, regulates the BES by enforcing reliability standards for the national electrical grid and regulating the wholesale electrical market (FERC 2014). While the President and Congress do not generally review FERC decisions, federal courts retain review power and the agency is subject to Inspector General audits. FERC is self-funded through annual fees that they levy on the industries they regulate (FERC 2010). FERC has the authority to implement civil penalties to ensure the reliability of the BES, prevent energy market manipulation, and provide rate incentives to promote utility transmission investment.[11] In short, FERC ensures that consumers have reasonable access to the energy resources they need and that electrical sector stakeholders are appropriately compensated. In coordination with the National Institute of Standards and Technology (NIST), the non-regulatory agency that helps to create national standards and advance technology, FERC also has the responsibility to coordinate the development and adoption of mandatory cybersecurity standards(FERC 2016). These standards, called Critical Infrastructure Protection (CIP) standards, require BES stakeholders to design incident response and recovery plans, which identify critical cyber assets, conduct vulnerability assessments, and install minimum personnel training controls (FERC 2008a).[12] Importantly, these standards are the only mandatory cybersecurity standards in place across all critical infrastructures of the U.S. and are enforced by federal statute (EEI 2014).[13] In 2006, FERC delegated to the North American Electrical Reliability Corporation (NERC) the authority to draft and oversee reliability and security standards, including cybersecurity, although it retained final approval for all standards that NERC put forward. The BES defines the outer limit of FERC and NERC reliability authority; they are complemented by PUCs, which focus on the non-BES (FERC 2008b).

[11] Fines are based on the severity level of the violation and cannot exceed $1,000,000 per day, per violation. FERC can also place non-financial punishments, such as limitations on activities, functions, operations, or placement of the violator's name on a reliability watch list of major violators.

[12] The CIP applies to not just critical infrastructure assets but any Cyber Asset, Electronic Security Perimeter, or communication system (i.e. critical infrastructure) that support the reliable operation of the BES at risk to cyber attack, including those at low, medium, or high risk.

[13] The Nuclear Regulatory Commission also requires cybersecurity standards for nuclear power.



North American Electrical Reliability Corporation

The North American Electrical Reliability Corporation (NERC) is a non-profit regulatory authority whose mission is to ensure the reliability of the BES in North America. NERC is self-regulated and self-funded; it is a non-governmental entity to which the governments of the U.S., Mexico and Canada have delegated power, and operations are funded by fees on BES stakeholders, like FERC. As described above, NERC is essentially the operational arm of the FERC. It develops and enforces electrical reliability standards, including cybersecurity. FERC is the approving entity but cannot draft its own cybersecurity standards; it can only make recommendations to the NERC. This means both must work together to implement policy. NERC also oversees several other entities, and hosts a number of cybersecurity-related events. NERC's role in cyber threat information sharing stems from its Electricity Information Sharing and Analysis Center (E-ISAC).[14] E-ISAC partners with various federal agencies, other industry ISACs, and the private sector to alert registered entities to timely security threats and provide mitigation guidance. If a vulnerability or threat is seen as significant to electrical reliability, NERC may even mandate BES stakeholder action. The NERC hosts regular electrical grid security events, such as GridEx and GridSecCon, bringing together cybersecurity experts from industry and government, allowing electrical sector stakeholders to test their resiliency measures and share emerging security trends, policy advancements, and lessons learned. The Cyber Risk Information Sharing Program

[14] Formally known as the ES-ISAC, Electricity Sector Information Sharing and Analysis Center.

(CRISP), a public-private partnership designed to facilitate the voluntary sharing of cyber threat information to amongst critical infrastructure owners and operators, the E-ISAC, and the DOE are all also managed by NERC. To enable information-sharing, CRISP volunteers install technology in their networks and sends encrypted data to the CRISP analysis center, which analyzes the data and sends alerts and mitigation measures back to the participants. CRISP, ISACs and ISAOs (Information sharing and analysis organizations), an emerging model for information sharing, are described in more detail below.

POLITICAL CHALLENGES

Unfortunately for the non-BES, many state public utility commissions, or PUCs, have not taken significant action to champion cybersecurity or provide resources to help offset costs (PUC Official 2-16 & 1-17). PUCs have had little involvement in promoting, incentivizing or mandating cybersecurity standards, "...pay[ing] scant attention to issues of grid security" (Koppel 2015). Most state PUCs have not created any cybersecurity recommendations for the distribution sector, (NARUC 2014; PUC Official 2-16 & 1-17) and some have even outright rejected the idea of performing any sort of cybersecurity oversight in favor of willful ignorance.

Surprisingly, these states appear to be wary of questioning the cybersecurity capabilities of utilities for fear of learning information that may compel them to take action or hold them legally responsible if they do not (NARUC 2014; PUC Official 2-16 & 1-17).[15] Further, some PUCs worry that sensitive and proprietary information they obtain could be subject to public disclosure, sunlight, or Freedom of Information Act (FOIA) requests. Commissions are hesitant to gather and store certain kinds of information because they are then responsible for keeping it safe. According to the National Association of Regulatory Commissioners (NARUC) and in interviews with PUC officials, "the line between knowing enough to determine that a utility's actions are prudent and knowing so much that the information held by the Commission can pose a cybersecurity risk is a line that commissions should walk carefully" (Keogh and Cody 2012; PUC Official 2-16 & 1-17). Unlike their traditional role of ensuring electrical power reliability, it is not clear in most states how PUCs are to carry out this task with regard to cybersecurity threats—but are a handful of states that are beginning to treat cybersecurity with the seriousness it demands.

One of the most advanced states providing cybersecurity oversight is New Jersey, whose PUC and Governor's office just last year drafted and approved cybersecurity requirements for the electrical sector (New Jersey Board of Public Utilities 2016). While these requirements are not proscriptive and are mainly focused on information gathering, they are a remarkable starting point. The requirements rightly identify cybersecurity as a high-level threat, and they require utilities to establish a plan to mitigate cybersecurity

[15] This was corroborated by the authors of this paper when talking to several PUCs, who wished to remain anonymous.

risks, keep records and report cyber incidents, monitor vendor security updates, promote cybersecurity awareness and training, and install reporting conditions to gather comprehensive awareness of the current state of cybersecurity (New Jersey Board of Public Utilities 2016). The requirements also cover the electric, gas, and water/sewer sectors, making them much more general in nature to the electrical sector than the federal standards discussed and recommended in this paper. They do however setup a framework to provide significantly improved state oversight and cyber incident planning. They also ensure integration with the state's information sharing entity, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC),[16] which in itself is an equally important achievement as most all states do not have an information sharing apparatus for cyber incident response.[17] However, perhaps most importantly, the New Jersey PUC (the New Jersey Board of Public Utilities) also allows utilities to pass approved cybersecurity costs to consumers through regular rate case process. Ultimately, states should endeavor to catch up to their New Jersey peer and implement these best practices.

PUCs could become one of the most important stakeholders in electrical sector cybersecurity as they have their hands on two very important financial levers: they decide a utility's return on equity (ROE), or what percentage of profits utilities can keep, and must explicitly authorize what investment costs can be passed on to the consumer, including cybersecurity investments. Using these incentives, PUCs could become one of the most influential stakeholders in promoting cybersecurity investments for the entire electrical sector. One reason for delay in cybersecurity investment is that PUC commissioners lack a decision-making process and adequate risk analysis information to allow utilities to recoup cybersecurity costs. To their credit, many PUCs realize that "cybersecurity remains an area where a lot of work needs to be done," and that they should bear responsibility to determine if utilities are making prudent investments in cybersecurity and if those investments are properly prioritized (Keogh and Cody 2012). In addition, not all of the responsibility for cybersecurity capacity building is on PUCs directly, as any mandate they have to improve cybersecurity is unclear at best. Ultimately, state legislatures and governors have the power to guide their mandate by clarifying their roles and responsibilities in state law. States could look first to involve their CIO and CISO.

It is important for state CIOs, and CISOs to be intimately involved in cyber incident preparation. Cybersecurity must not be a patched afterthought or housed solely in a separate stovepiped agency, but fully integrated into the operations and culture of the entire state government enterprise. During an incident, CIOs take on a critical role of disseminating cyber threat information among government agencies, working closely

[16] In 2015, pursuant to Executive Order No. 178, the Governor established the New Jersey Cyber Security and Communications Integration Cell (NJCCIC) under New Jersey Office of Homeland Security and Preparedness to coordinate cybersecurity information sharing between the government agencies and the private sectors.

[17] Information sharing and state capabilities are covered later in this paper.

with state emergency services offices to provide technical assistance. However, the job of the CIO is difficult, not only in corralling a disparate group of stakeholders, but also in obtaining proper resources to accomplish their mandate. A survey of CIOs showed that 75.5 percent of CIOs lack sufficient funding to implement adequate cybersecurity. Because much of state government is moving to more efficient cloud providers, cybersecurity of state networks and public-private partnerships become even more critical to security efforts.

RECOMMENDATIONS

- Governors should designate a Cybersecurity Coordinator or elevate their State CISO to act in this capacity. Research for this paper found that very few senior state officials had basic cybersecurity knowledge or had directed any significant action to improve it. Much like state energy officials who engage in bettering state energy needs across all policy issues to provide whole of government oversight, states would also benefit from a governor-appointed cybersecurity leader. The federal government recognized this need and in 2011, then-President Obama appointed the Special Assistant to the President and the Cybersecurity Coordinator. The state Cybersecurity Coordinator (or leader by another name) should borrow from both models, leading interagency development and implementation of cybersecurity strategy and policies, with a complete view of the economic and national security matters. They should begin by leading the development and implementation of an interagency cybersecurity strategy and policy, ensuring close partnerships with the federal government and private sector. A special focus should be given to state emergency management officials to aid in cyber incident response for high-risk events, who—to aid in planning efforts—should be required to include applicable cybersecurity standards, incident response and information sharing policies in state Energy Assurance Plans. States could request DOE funds to include cybersecurity in Energy Assurance Plans, as was done in 2009.

- Each state Cybersecurity Coordinator should have a direct line of communication and interact regularly with the federal Cybersecurity Coordinator to plan and strategize for cyber incidents that threaten national security, as well as share best practices. This model would provide an important communication hotline between state executives and the White House for significant cyber events, and could be especially useful for populous states with immense, complex systems. To be clear, the Cybersecurity Coordinator should be empowered to act not just in incident response but in all areas of cybersecurity and policymaking. Moreover, state Coordinators could aid governors in taking advantage of current DOE and DHS cybersecurity grant opportunities, which are currently far underutilized. For example, FEMA's non-disaster preparedness grants can be used to enhance the capacity of state and local emergency responders to prevent, respond to, and recover from cyber-attacks.

- To protect PUCs during audits and collection of information, necessary legal protections should be afforded for handling and storing critical infrastructure and cybersecurity information, such as that which includes personally identifiable and proprietary information, and should restrict public disclosure requests, as is done in several states. States should undertake a legal review to see if protection from FOIA requests is required or if a federal legal privilege preempting state disclosure requirements should be created. To be clear, any new information PUCs deem necessary to store on their systems must be secure. States could model the use, storage, and destruction of sensitive or proprietary information after other critical infrastructure sectors, such as the financial sector. States should also design laws that assign liability on the basis of CIP adoption to catalyze adoption of these basic cybersecurity standards. An entity that does not meet these standards could be found negligent for failing to take actions to limit the consequences of a cyber incident.

CYBERSECURITY INFORMATION SHARING

Cybersecurity Information Sharing consists of the passing of relevant, high quality threat and compromise information to a group of stakeholders that can then ingest and utilize said information to help harden their networks and reduce the risk of malicious network compromises. Access to this high quality cyber threat information is the keystone for electrical sector protection. It allows participating non-BES stakeholders to address evolving threats, enabling quick and anonymous sharing of sensitive, proprietary, and classified information to bolster resilience to cyberattacks, ensure situational awareness during incidents, and disseminate best practices to better understand attack vectors (Ridge and McLarthy 2014). While the concept is relatively simple in theory, it is in practice to rife with legal and privacy issues, information quality concerns, policy and political challenges, and a general lack of cost efficiency and resourcing. All of these inhibit real-time sharing of high-quality cyber threat information amongst non-BES stakeholders and government entities. Each of these concerns must be addressed in order to entice non-BES stakeholders into participating and utilizing cybersecurity information.

THE NEED FOR HIGH QUALITY INFORMATION

Equally as important as sharing information is the quality of the information that is shared. Information does little good to the end user unless it is actionable and pertinent, meaning that the utility customer must be able to use the information being shared with them and it must be something that pertains to their individual specific network or configuration. While information quality is a simple concept, it is notoriously hard to execute; each non-BES utility can in effect have a unique network setup employing network protocols and equipment not found elsewhere.

These inconsistencies mean that without a customizable data-stream of cybersecurity threat information, utilities are instead required to sift through potentially enormous

amounts of data to find the information that they need, which in turn dramatically increases the time it takes to harden their networks against emerging threats and also heightens resource drain in a likely resource-scarce environment. This impediment greatly reduces the participation of stakeholders in information programs, which in turn reduces their efficacy as more and more utilities largely ignore, or in some cases simply decline to use, information services.

This paper defines the quality of information based on the essential factors of usability and availability, both of which are dependent upon the following:

1. Standardization: All parties are speaking the same language and transmitted information is comprehensible and repeatable (Connolly, Davidson, and Schmidt 2014).
2. Rapid and Continual: Threat and vulnerability information loses value over time, so the process should be as expedient as possible while maintaining quality.
3. Multidirectional: Information must flow between industry and government as well as amongst industries equally, so that potential end users are not excluded or limited in any scenario (Inserra and Rosenzweig 2014).
4. Actionable: Information that involves present threats or vulnerability and demands corrective action must be prioritized over other forms of information (EEI 2014, 4).
5. High Fidelity: Information needs to be inspected so that disruptive or damaging errors (i.e. false positives) can be addressed.
6. Industry-Specific: Threat and vulnerability information does not apply equally to different industries; for example, threats to point of sale systems are significantly more valuable to retailers than a utility.
7. Source of Intelligence: The sources of cyber threat information must perpetually provide a wellspring of relevant information, because poor sources will bear little fruit; accordingly, public and private information sharing facilitators must be interconnected and private non-BES stakeholders incentivized to participate.

While there are some exceptions, non-BES stakeholders tend to be resource-constrained both in their budget and available human capital. Accordingly, even if all the legal and policy concerns have been addressed and high quality information is available, there remains a risk that the information would not be usable simply due to the lack of manpower. Rapid technological advancements have made the process increasingly efficient, easier to implement, more secure, and most importantly, cheaper. Contemporary information sharing structures possess near ‘real-time’ information sharing capabilities, so that as sectors receive relevant information, almost immediate transmission to the appropriate recipients occurs. They also emphasize usability, managing gross amounts of data and sorting pertinent, actionable information from irrelevant information quickly and accurately (Ridge and McLarthy 2014).

INFORMATION EXCHANGE PLATFORMS

One key component from the above list is standardization. Fortunately, this area has been improved measurably over the last few years due to the Trusted Automated eXchange of Indicator Information (TAXII) program and the complementary Structured Threat Information eXpression (STIX) standardized platform, and the Cybersecurity Risk Information Sharing Program (CRISP). While improvements and rollout are still underway, the systems are showing potential to cut down on inefficient labor costs, improve the value of raw data exchange, and simplify and speed up the process of cyber threat information exchange (Jackson Higgins 2015).

STIX

The Structured Threat Information eXpression (STIX) is a collaborative, DHS-led effort to develop a standardized language representing cyber threat information and cyberattack indicators (MITRE, n.d.). The intent of standardization is to allow the widest possible community of information sources to share and receive cybersecurity information without translation hurdles in both a "human-readable" and "machine-parsable" manner (MITRE, n.d.). Currently, automated management and exchange of cyber threat information is tied to specific security product, service, or community-specific languages. STIX enables the sharing of cyber threat information across organizational, community, and product/service boundaries.

While the STIX language itself is still in development by its open-source partners, many organizations have already begun incorporating it into their processes. The DHS Cyber Information Sharing and Collaboration Program has started using STIX for its operational threat information to partners. The NCCIC is phasing STIX into its cyber threat informational products. The FS-ISAC recently became the first ISAC to utilize STIX in its information sharing mechanisms (MITRE, n.d.). In other words, automated information sharing requires an agreed upon method of sharing; the STIX method is primarily partnered with TAXII, an automated information sharing vehicle.

TAXII

The Trusted Automated eXchange of Indicator Information (TAXII) is a cyber indicator delivery vehicle that enables sharing of cyber threat information across organization and product or service boundaries. TAXII itself is not a specific information sharing application, and does not impose its own design on users; instead, it can be layered on top of existing data management processes (MITRE, n.d.). TAXII is also a DHS-led effort intended to facilitate the sharing of cyber threat information with many sharing partners through automated, standardized message exchanges which eliminates the need for custom sharing with each partner (MITRE, n.d.).

With TAXII, cyber security threat information sharing is faster, as the automation has replaced most of the manual undertaking. TAXII also increases the security and privacy

of threat indicators by reducing the technical hurdles and steps needed to participate in threat sharing (Connolly, Davidson, and Schmidt 2014). The effort previously directed towards the manual creation of threat indicators can now be used to analyze them, and vendor products and services can use TAXII to achieve interoperability with other TAXII-enabled software.

INFORMATION BROKERS AND FACILITATORS

There has never been a greater need for information sharing between key stakeholders. However, too many providers of information can be problematic; one example is the current proliferation of information sharing facilitators or brokers, the largest of which are government-based. According to interviews for this paper, non-BES stakeholders by and large argued that no two facilitators used the same information brokers, and all operators had their own opinions about the relative usefulness of each of the services to which they subscribed.

This is not to say that all facilitators are bad; indeed, many have been lauded as tremendously valuable. It is simply important for non-BES stakeholders to both understand which of these organizations can help address their needs and what each one does. A few of the more well-known efforts and organizations follow.

NCCIC

The NCCIC is the primary arbiter of information sharing amongst critical infrastructure information facilitators, among other roles. DHS, via the NCCIC, provides a platform to share alerts, indicators, and information about previous attacks, threat actors, and threat signatures regarding critical infrastructure. Threat information can include tactics, techniques, and procedures used by an adversary; the target or vulnerability the enemy is trying to exploit; evidence that shows an attack to be part of a campaign of cyberattacks; indicators that point to a certain hacker or type of hacker; and courses of action to mitigate or fix cyber vulnerabilities (Connolly, Davidson, and Schmidt 2014). Receiving a continual flow of this information allows cybersecurity professionals to coordinate policy to improve resilience and reliability. The NCCIC works with entities at the federal, state and local levels, including law enforcement, to monitor critical infrastructure and to prepare, mitigate, and provide technical assistance to cyber threats and vulnerabilities. This includes providing states information on the electrical sector via partner information facilitators, including fusion centers, ISACs, and ISAOs.

Fusion Centers

Currently, central conduits of cyber threat information to states are fusion centers, which may not be ideal. They were created after 9/11 to focus on sharing antiterrorism intelligence across federal, state, and local agencies. Since then, fusion centers have expanded their role in traditional information sharing amongst law enforcement communities to include the growing challenges presented by cybersecurity, which require a completely different and more advanced system to share information. Fusion centers are owned and operated by state and local governments but federally subsidized, and they

serve as focal points to receive, analyze, and share threat-related information. States use fusion centers to receive and utilize threat information from the NCCIC, various ISACs, ISAOs, and regional partners (NGA 2015).

Today, fusion centers are seen as lacking the proficiency to share timely, high-quality cyber threat information, although progress is being made to improve capabilities. To date, there are 78 fusion centers in the United States—53 are owned and operated by states and territories, and 25 by major urban areas (NGA 2015). Unfortunately, fusion centers have been "of uneven quality—oftentimes shoddy, rarely timely, [and] sometimes endangering citizens' civil liberties and Privacy Act protections," according to a 2012 report by the U.S. Senate Permanent Subcommittee on Investigations (U.S. Senate PSI 2012). As a result, while fusion centers are supposed to be a key federal to state conduit for cyber threat information, they may be far more focused on preventing traditional acts of terrorism than building cybersecurity capabilities. The combination of demands of their primary mission and limited resources may prevent fusion centers from focusing on building out cyber defense capacity and providing specialized service to certain industries (NGA 2015). In fact, a report commissioned by the Department of Justice and Homeland Security acknowledged that at least some fusion centers have "limited cyber knowledge" (Global Advisory Committee 2015). Fusion centers are in the nascent stages of building their cyber threat information sharing capabilities and capacities, mainly relying on a single onsite Cyber Liaison Officer (NGA 2015). One positive development is the creation of the Fusion Center and Fusion Liaison Officer Cybersecurity Toolkits by DHS, which help to enhance the cybersecurity resources available to fusion centers and liaison officers (NGA 2015).

Information Sharing and Analysis Centers (ISACs)

In 1998, President Bill Clinton issued Presidential Decision Directive 63, which called for the establishment of an ISAC for each of the eight infrastructure industries deemed critical to the national economy and public well-being (The White House 1998). The communications, finance, water, aviation, transportation, law enforcement, health, energy, and natural resources sectors were all encouraged to start their own ISAC programs (The White House 1998). ISACs are nonprofit entities established by critical infrastructure owners and operators to provide sector-specific cybersecurity analysis through shared information and threat indicators. This shared information is distributed to the ISAC's private members, to other sectors, and to the federal government. Most of the nation's ISACs are organized under the National Council of ISACs, a group that promotes information sharing and defensive cohesiveness (NCI 2017). The Council's activities include drills and training exercises, hosting a private sector liaison at DHS, and sponsoring events to bring together the critical infrastructure community for training and preparedness. These information sharing relationships are strengthened by partnerships with DHS's United States Computer Readiness Team (US-CERT), a division of the DHS National Cybersecurity Communications Integration Center (NCCIC) (NCI 2017).

ES-ISAC

The energy sector's ISAC is unique in that it is operated by NERC on behalf of the electrical industry, as described above. This ES-ISAC serves as the central coordination hub for cyber and physical risk information sharing across the electricity sector (E-ISAC 2017). Formed in 1998, its primary function is the rapid sharing of information regarding real and potential security threats, as well as the methods and tools to avoid or mitigate the impact of an attack.

The ES-ISAC develops security alerts and notifications for distribution to registered entities. It gathers information from industry participants about security-related events, disturbances and off-normal occurrences, and shares that information with its partners and the government. In turn, the government provides information regarding risks, threats and warnings to the ES-ISAC, which is responsible for disseminating that information to partners (E-ISAC 2017). The alerts are categorized into three levels: advisories, which are purely informational and do not require a response; industry recommendations, which endorse 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.

The ES-ISAC maintains a seat on the NCCIC to provide actionable private energy sector cyber threat information and indicator analysis, including to and from the non-BES (NERC 2014b). To prepare electrical sector stakeholders, the ES-ISAC runs Cyber Risk Preparedness Assessments (CRPA), which assesses their cyber response capabilities. Stakeholders gain a better understanding of their cybersecurity programs, which allows them to identify potential areas of improvement. NERC is also responsible for enforcing violations of its reliability standards[18] and facilitating sensitive information sharing. Some have advocated for the ES-ISAC to be spun off into a separate entity to avoid conflicts of interest and better willingness to share information (Michael Hayden, Curt Hébert, and Susan Tierney 2014).[19] This paper endorses this recommendation in the context of the goal of establishing industry-led solutions operating under responsible government oversight (Inserra and Rosenzweig 2014).

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The Multi-State ISAC is the epicenter for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments. As a part of the nonprofit Center for Internet Security (CIS), the MS-ISAC provides network monitoring, early cyber threat warnings, threat indicators and cyber information sharing, along with advisories, vulnerability identification and mitigation and incidence response

[18] Penalties can range upwards of $1 million per day; see the Standards section of this paper

[19] Consequently, in part, E-ISAC does not match the analysis capabilities and current potential of the Financial Sector ISAC. Energy sector and government officials agree that, "the rigor, maturity and complexity of what is being done in the electricity sector are significantly less than in the financial sector" (Behr 2014). However, the electrical sector is considered to be amongst the most sophisticated, particularly because of the relative strength of their regulatory environment and the focus of industry executives.

to its members (CIS 2017). All 50 states are represented in the MS-ISAC (CIS 2017). In addition to states, many local, tribal, and territorial governments are active members. For example, the state of California is represented by the CIO of the state, but also has 61 cities and counties as well as a single tribe with full membership status (CIS 2017). The MS-ISAC also includes representatives from state homeland security offices, as well as law enforcement and others in the physical security field (CIS 2017). MS-ISAC is a primary part of the NCCIC; in fact, the NCCIC floor has several desks devoted to MS-ISAC information sharing activity.

MS-ISAC members receive numerous cybersecurity benefits. Members are provided with cyberattack incidence response technical assistance, cybersecurity advisories including notifications about potentially compromised systems or software, training opportunities and best-practices, bi-monthly expert webcasts and monthly member webcasts, access to secure portals for email and document sharing provided by US-CERT, a cybersecurity alert level status map for each state, monthly calls with vendors to learn about software patches and updates, and an annual member conference featuring expert testimony and training (CIS 2017). In addition to that role, the MS-ISAC is beginning to provide fee-based services, including network monitoring, vulnerability scanning, and penetration testing. In order to receive these benefits, members agree to share cybersecurity information and protect the sensitivity and confidentiality of any information shared; yet because there is no requirement to participate at any specified level, engagement from members varies. Similarly, the MS-ISAC makes no guarantee on the accuracy or reliability of the information shared on the platform.

Information Sharing and Analysis Organizations (ISAOs)

On February 13, 2015, then-President Obama signed Executive Order 13691 to promote private sector cybersecurity information sharing by encouraging the creation of ISAOs (The White House 2013). The Order directs DHS to set voluntary standards for ISAOs and streamlines the mechanisms that the NCCIC uses to enter into voluntary information sharing agreements. Participants in an ISAO can request that their information be treated as protected critical infrastructure information (PCII), which is confidential, and exempt from regulatory use or civil litigation (DHS 2016a). It also adds DHS to the list of federal agencies that can approve classified information sharing arrangements to ensure ISAOs can access valuable classified cybersecurity threat information held by the federal government.

ISAOs can be any nonprofit group, membership organization, or single entity that serves as the focal point for cybersecurity information sharing and collaboration, both within the private sector and between the private sector and the government (DHS 2016a). Currently, most private sector information sharing is conducted through ISACs operating on a sector-by-sector model using only the collective information of sector-specific companies, most of which deal in critical infrastructure. ISAOs, on the other hand, provide more flexibility and the necessary means for information sharing between

companies that do not fit neatly into an established sector and therefore cannot join an ISAC (DHS 2016a). However, ISAOs (and ISACs) share threat information with DHS, allowing cyber threat information to be shared between industry sectors (i.e. information on an attack on the banking sector will be shared with the electrical sector).

For private entities, ISAOs work much the same as ISACs in the way that they share cyber threat indicators or other information among their members. For government organizations, ISAOs will have their information sharing processes dictated to them from the DHS-designated nonprofit standards-forming organization. While that process is in its nascent stages, it is clear that the NCCIC will engage in coordination with ISAOs that wish to collaborate in voluntary information sharing agreements with the government. The new process will also address how ISAOs can share with ISACs, thereby broadening each group's cybersecurity information network (DHS 2016a).

CRISP

The Cybersecurity Risk Information Sharing Program (CRISP) is an automated and voluntary data-sharing program that utilized private sector intelligence and technology. The pilot has gained some popularity in the utility industry. CRISP aims to facilitate the sharing of cyber threat information in the electrical sector by providing near real-time capability for electrical critical infrastructure owners and operators to voluntarily share cyber threat data and receive additional government indicators and intelligence via an automated machine-to-machine connection. CRISP is a partnership between the DOE's Office of Electricity Delivery and Energy Reliability (DOE-OE), the ES-ISAC, the Pacific Northwest National Laboratory (PNNL), and other participating private stakeholders (NERC 2014a). The ES-ISAC is the program manager, and oversees the installation and maintenance of the hardware that CRISP utilizes (NERC 2014a). CRISP has three main technological elements: the Information Sharing Device (ISD), the Cyber Fed Model (CFM) and the Contested Operations Network for Reporting and Detection (CONRAD). Together, these elements provide CRISP the ability to analyze and exchange cybersecurity threat information in a reliable and secure way. DOE is continuing to develop CRISP by incorporating two additional national labs and the National Science Foundation is currently soliciting additional private partners to assist (NSF 2016).

Institutions that participate in CRISP install the Information Sharing Device (ISD) in their network just outside the corporate firewall (NERC 2014a). It collects data and sends it in encrypted form to the CRISP Analysis Center at PNNL. The Center analyzes the data and sends alerts and mitigation measures back to the participating companies about potential cybersecurity breaches; the Center also does the same for any alerts it receives from the government or the ES-ISAC. These alerts are used by stakeholders' intrusion detection or prevention systems to thwart malicious activity. While this architecture would be able to intercept IT threats attempting to traverse to ICS networks and specific ICS network threats that tried to connect to the outside via egress communications, it did not necessarily cover insider or boundary skipping threats. This meant that computer

malware threats such as HAVEX , which could utilize trusted Virtual Private Network (VPN) connections, or threats such as USB sticks or vendor laptops such as was likely used in STUXNET. Accordingly, a majority of the high-impact custom threats to ICS were not necessarily addressed.

The CFM is a software program installed on a site's computers, which enables them to exchange cyber threat information with other CFM sites. It includes encryption-based information exchange protocols to determine those allowed to receive and access the data. In addition to the reports and analysis, the CFM shares hostile IP addresses and domains, and other threat indicators every five to fifteen minutes in an automated machine-to-machine capacity to help with cyberattack prevention (NERC 2014a). The CONRAD device and communications network allows a compromised site to coordinate with other sites to mitigate the threat in a secure way without the perpetrator knowing about the communications. In this way, a site that has been attacked will alert the other sites in the electrical system, which will then have time to engage in defensive maneuvers. Because of these proprietary features, CRISP has become the preferred technology in DOE and the electrical sector.

RECOMMENDATIONS

- Establish and Empower a State Integration Center or Information Sharing Hub. In order to advance information sharing, states must establish an information sharing entity that serves state priorities exclusively. Nationwide information sharing entities do not filter information to fit the particular needs of states, taking into consideration of resources and vulnerabilities unique to the state. Cyber incidents also originate from within states, so having a robust system to supply new threat information to the national information sharing entities such as the NCCIC is highly advantageous. As states build capacity, they will also inherently build security-minded relationships with private actors that are beyond what distracted and unfocused fusion centers can accomplish. Cybersecurity challenges are constantly evolving, and integration centers are needed to process shared information, analyze it and make it actionable, and distribute it to state partners. Implementing future policy changes will rely upon this centralized, coordinating capability. To date, three states have accomplished this, and three others are in the planning process (Spidalieri 2015).

- Encourage Information Sharing Through Existing Platforms Such as Fusion Centers and the MS-ISAC. States need to take steps to encourage stakeholders to use existing information sharing platforms in the absence of, and eventually including, a state integration center. Generally, state governments are not well equipped to contextualize threat information they receive and tailor it to meet their own needs. Fusion centers and the MS-ISAC can perform that essential function by providing analyses of the threat intelligence they receive and disseminate. Ways of enhancing fusion centers include expanding access for key state operators, assessing and communicating capabilities, establish performance

measurements, and developing a strategic operations plan involving regional stakeholders in all phases of a cyber incident (preparation, incident response, and forensics). Fusion center capability will help states integrate their law enforcement efforts regarding cyber-crime. Regardless of the existence or relative strength of a state's integration center, fusion centers will continue to be a critical resource in investigating cybercrime and engaging the state's law enforcement resources. Similarly, robust participation in the MS-ISAC is necessary for an individual state to access valuable intelligence that may be generated by other states.

- Information Quality. Last and most importantly, states should ensure the high quality of cyber threat information using the seven factors of information quality defined in this paper as metrics. High quality information is the foundation of an effective information sharing system; without it, the infrastructure and partnership building, budget investments, and human capital promoted through various policies will be for naught. Information sharing facilitators (ISACs, ISAOs, MS-ISAC, fusion centers, industry groups, government, etc.) must set clear principles for information quality that are well understood and prioritized. These include making the information sharing standardized, rapid and continual, multidirectional, actionable, high fidelity, industry-specific, and well sourced. States should empower a task force or commission with authority to oversee the information sharing operations, public and private, within a state and work to promote information quality based upon these principles. That body should also produce public annual reports tracking their efforts to improve each of these information quality factors and identify areas for improvement.

PRIVATE SECTOR AND STATE COOPERATION

The need for more robust partnerships, real-time coordination and response planning has never been greater for both public and private power generation and distribution companies that try to address cybersecurity threats alone are bound to fail (Lohrmann 2014). The private sector has a multitude of additional policy concerns, which complicate information sharing systems aside from the main challenge of collecting and using cyber threat information. While barriers exist, efforts to establish effective information sharing channels among private entities and industry clusters are critical.

The private sector's hesitation to share information is deeply rooted in fears over the threat of lawsuits, regulatory penalties, liability concerns, antitrust issues, lack of a business incentive, and general mistrust. While recognizing the need for information sharing, private industry has particular concerns about liability protections. Private entities fear that information shared with government could be subject to a public records request, result in the forfeit of certain intellectual property rights, be used for regulatory action, or risk the privacy rights of individuals whose information may be included in

disclosed information (Nolan 2015). Beyond this, sharing amongst private sector partners also raises a variety of potential legal scenarios involving state privacy laws, antitrust laws, tort law, as well as law regarding stock corporations, shareholders, and elements of the Uniform Commercial Code (Nolan 2015).

Additional limiting factors to, and a general reluctance to participate in, the current information sharing system can also be attributed to potential regulatory compliance requirements and public disclosure rules for those who do participate. This fear among potential information sharing participants, such as non-BES stakeholders, still exists despite recent federal efforts (Campbell 2015). For example, information shared between non-BES stakeholders and state agencies, such as PUCs, could be subject to public disclosure laws, providing a perverse disincentive for non-BES stakeholders to abstain from sharing critical cyber threat information (Keogh and Cody 2012).[20]

Fortunately, there has been some progress in resolving policy and legal issues. Executive Order 13691 encouraged individual states to accelerate information sharing with private sector entities and facilitate the improved exchange of people, data, resources, and trust. Eight states (California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington) have set themselves apart in addressing cybersecurity information sharing through executive action, policymaking, or investment. Michigan, Virginia, New Jersey, New York and California have all launched their own state-operated information sharing hubs and are working to establish online platforms to facilitate incident reporting and real-time sharing (Spidalieri 2015). Notably, California's Executive Order creates a new state-operated Integration Center and a Computer Incident Response Team (CIRT), which will utilize the capability of various stakeholders such as DHS, academic institutions, federal law enforcement, and, importantly, the National Guard (Brown 2016). Nonetheless, resources to improve information sharing and to address cybersecurity in general remain an issue at the state level.

PRIVATE SECTOR LEGAL PROTECTIONS

Another advancement to solving information sharing policy and legal issues took place in 2015, when the first piece of significant cybersecurity legislation after more than a decade was passed into law: the Cybersecurity Information Sharing Act (CISA). While the law only took a few elements from previous versions over the past three years, it was finally passed as a part of the yearly must-pass funding bill over the objection of some business and privacy groups (Greenberg and Grauer 2015). According to its Senate authors, CISA "creates an environment that encourages the sharing of information about cyber threats, allowing all participants to get a better understanding of the current threats that may be used against them" (U.S. Senate PSI 2015).

The law, in general, promotes voluntary information sharing of cyber threat indicators (e.g. malicious software, Internet protocol addresses, or even emails) among private companies and between the private sector and government through liability protections

[20] See the Standards section of this paper for further discussion.

for those that share or use cyber threat information. The protection prohibits legal action against an entity that acts in good faith to act on shared cyber threat information, shares cyber threat information, or chooses not to share information, in accordance with the law. CISA also codifies the NCCIC and its role as the lead federal information sharing clearinghouse, or "portal" for cyber threats between government and non-government entities. Moreover, the law aims to protect individual privacy by requiring private companies and also DHS to remove personally identifiable information from the information they share. Data shared with the NSA must pass through or emanate from a federal source, such as DHS, which will also share classified and unclassified cyber threat indicators and defensive measures, including with appropriate private entities such as critical infrastructure operators. CISA allows specific categories of cyber threat indicators to be shared, including: cybersecurity; investigation and prosecution of a specific threat of death, physical injury, or serious economic harm; protection of minors from sexual exploitation; and the investigation and prosecution of espionage and cybercrimes.

Of particular note is that the law is completely voluntary and provides no government surveillance authority, even if a cyber threat includes information relevant to a criminal investigation. To force a future review of the law's provisions, CISA includes numerous reporting requirements and, absent congressional action, becomes void after 10 years. However, regulatory and public disclosure concerns and implications for privacy and property rights may still exist at the state-level depending on the interpretation of state law. As of this writing, CISA is being interpreted by states and may preempt some state efforts that go beyond or have similar requirements.

State legislation can help codify liability protections and extend an understanding of the policy and its intent to stakeholders. Much of the information sharing policy debate has occurred in Congress, dominated by high-level industry representatives and privacy advocates. State-level actors such as non-BES stakeholders can benefit from outreach and training on how information sharing is no longer a trade off and makes business sense for private companies of all sizes. Many state legislatures have a difficult time incentivizing information sharing under existing regulatory structures, so efforts to inform private actors should be taken. For example, last year, the Department of Justice (DOJ) and Federal Trade Commission (FTC) issued a joint statement clarifying that industry would not be liable for collusion or antitrust violations for sharing relevant cyber threat information (DOJ and FTC 2014).

What is often not discussed is that private actors can utilize traditional legal methods of reducing liability, such as contracts, asset reclassification, or different forms of incorporations. For example, the limited liability company (LLC) model is often used to protect principal ownership from liability. In the cyber context, information travels from utilities to an LLC before making it to the relevant ISAC. This has been widely recommended as a means of addressing concerns about liability, anti-trust violations, and

information leaks. In the electrical sector, participants note the LLC model has so far been used by only a few electrical utilities (Ridge and McLarthy 2014).

PUBLIC PRIVATE PARTNERSHIPS

Another development at the state level is the practice of labor exchange between industry and the public sector as a way to build expertise and to reduce costs. Workforce exchange programs, in which government employees temporarily work in the private sector and vice versa in relevant state departments, allow participants to understand the challenges unique to the public and private sectors. In its 2011 Strategy for Operating in Cyberspace, DOD explicitly endorsed "[labor] exchange programs to allow for 'no penalty' cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent." This type of labor exchange is perhaps the best way to address two major challenges: understanding the value that government resources can offer to industry, and shedding light on how cybersecurity is viewed in the context of corporate decision-making. Most importantly, state governments may be in the best position to facilitate labor exchange programs, using resources such as their public utility commissions, state university systems, or the National Guard.

RECOMMENDATIONS

- Commit to Forming Public-Private Collaboration and Labor Exchanges

    - *PPP Collaboration*: States must take steps to strengthen information sharing channels between government and the private sector, as well between different private sector organizations. States need to approach this goal through both formal and informal means, such as contracts or MOUs, as well as legislation granting appropriate authority and use of information. This should be done through strong incentives or by introducing compulsory regulations if needed. States must also take steps to define roles, expectations, and legal concerns, and remove any real or perceived barriers to entry. These barriers can include the costs of sharing information, which can range depending on the size and business model of a particular entity, and the challenge of recruiting, training, and retaining qualified personnel.

    - *Labor Exchanges*: The use of labor exchange programs to partnerships between the public and private sectors, such as those advocated for by DOD, should be expressly required by fiat. Governors and PUCs should require BES and non-BES stakeholders to develop labor exchanges to strengthen capabilities and build reciprocal understanding and trust amongst their cybersecurity workforces. Sharing information about an incident runs counter to the culture of most large organizations, but labor exchanges will begin to change the type of thinking that leads both public and private entities to react by first concealing information to reduce consequences. In the cybersecurity context, that thinking could be counterintuitive or even counter-productive.

- Promote Hunting for Network Compromises as well as Response Activities. Relying only on static defenses is not enough to provide reliable cybersecurity. Results from a 2014 real world test conducted by FireEye indicated that organizations that employed passive defense were breached 97 percent of the time by hackers (FireEye 2014). Intelligence sharing, while a keystone of any good cybersecurity program, and an effective workforce are not enough to stop malicious attacks. Electric companies must also rely on proactive measures, such as advanced hunting techniques, in order to ensure that they are adequately protected. Accordingly, states should encourage these companies to either hire or develop a hunting capability for their critical systems—preferably pooling resources across multiple companies whenever possible to allow for greater economies of scale.

ESTABLISHING STANDARDS

Unfortunately, the electrical sector may lack the incentive to expend sufficient resources on cybersecurity (Palmer 2010), suggesting that a market failure exists. In other words, non-BES stakeholders may be ignoring their cybersecurity risk (Grady and Parisi 2011). Senior DOD officials agree with this viewpoint; according to then Deputy Secretary of Defense Ashton Carter, "cybersecurity is underinvested, there's a market failure in cybersecurity" (Ashton Carter 2013). Government should take steps to correct market failures and promote cyberspace as an efficient, safe public good by filling the security void caused by insufficient market incentives (Lute and McConnell 2011). Identifying standards and best practices for cybersecurity can be an effective way to promote private sector security.

Employing some level of cybersecurity standard is important for all critical infrastructure operators, be they mandatory or incentivized. Part of the difficulty with current federal oversight is that much of electrical sector infrastructure is privately owned and federal policy dictates that critical infrastructure operators manage their own risks.[21] Government facilitation of standard adoption could play a key role in in helping to correct market failures.

While it is important to remember that standards are not a panacea—they do not incentivize improvement and adaptation to respond to all rapidly evolving cyber threats—they do help normalize cybersecurity activities, create economies of scale to reduce costs, highlight best practices, help facilitate cyber insurance, reduce the risk of moral hazard and government reliance, and provide a useful baseline. Baseline standards provide minimal but not insignificant protections and direction for future development. For example, the cascading outages of the 2011 Southwest Blackout "may have been avoided" if federal BES standards applied by the NERC had been applied to the non-BES distribution systems that failed (Bogorad and Nurani 2012). The importance of baseline standards are explicitly recognized in the President's Executive Order 13636, which directed the National Institutes of Standards and Technology (NIST) to develop its "baseline framework to *Reduce Cyber Risk to Critical Infrastructure" (The White House 2013).*

Determining the appropriate way to implement baseline standards, mandatory or incentivized, is industry and organization specific. The military is most concerned with accomplishing their mission and minimizing safety and security risks, so it implements mandatory cybersecurity standards and upgrades with less regard for cost. However, the same level of mandate may not be appropriate for private industry, including non-BES stakeholders, whose investment in cybersecurity must include a return on investment.

[21] Per PPD-21, "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient" (The White House 2013).

Based on an analysis of risk, cost, and political feasibility, this paper recommends a mixture of 'carrot and stick' measures to significantly improve electrical sector cybersecurity.

RECOMMENDATIONS

- States should require NERC CIP baseline standards. States should direct or legislate their public utility commissions, or PUCs, to require the adoption[22] of the NERC CIP cybersecurity standards by non-BES stakeholders. The new standards are routinely updated, effective, and used an industry collaboration model[23] to help ensure they are not onerous on private business. Based on analysis, allowing states to implement these standards on the non-BES rather than charging this responsibility to NERC provides them flexibility to customize the standards to specific state needs while still maintaining the effectiveness of the CIP standards. Performance criteria should be tailored for individual non-BES stakeholders, taking into account their risk of failure to the larger BES. Prior to implementation, states should conduct a comprehensive risk assessment to allow their PUCs to allocate resources appropriately over time. Non-BES stakeholders should also complete a cybersecurity risk assessment, using the NIST Framework, to evaluate what level of cybersecurity protections are appropriate for their companies. PUCs could assist in this effort if needed, aided by DHS and NIST, which currently provide technical resources to help perform this assessment and cover additional costs. Ultimately, the CIP standards, if implemented over a reasonable timeframe, provide the least hardship on private business and least cost to state governments while still achieving the most effective baseline cybersecurity protections available. To enforce these standards, states should consider financial penalties, as the NERC does.[24] And finally, PUCs should also join the NERC Critical Infrastructure Protection Committee to provide input on future CIP versions.

---

[22] Confirming the adoption of the CIP standards for grading is key. States should require PUCs to randomly audit utilities to confirm adoption of the standards. In the course of research for this paper, it became clear that utilities, through private cybersecurity assessment companies, were able to self-assess their compliance with mandatory NERC standards. While this may be necessary for the majority of compliance, the threat and execution of random audits will incite better adoption of the standards. In fact, incorrect self-certification of electrical sector standards has proven to bring serious consequences. One of the reasons for the 2011 Blackout was because BES entities were not in compliance with baseline NERC standards; the Arizona Public Service Company was fined $3.25 million by NERC standard violations (NERC 2014). The latest CIP standards is version five.

[23] NERC standards are ANSI accredited, ensuring collaboration with private industry. According to NERC and the non-profit ANSI, "the process is open to all persons who are directly and materially affected by the reliability of the North American bulk power system; transparent to the public; demonstrates the consensus for each standard; fairly balances the interests of all stakeholders; provides for reasonable notice and opportunity for comment; and enables the development of standards in a timely manner" (ANSI 2016).

[24] NERC fines for noncompliance with the CIP standards can be as much as $1 million a day.

- States should take advantage of tools the DOE offers to mitigate the lack of cybersecurity expertise of PUC personnel. For instance, the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) is a DOE tool that could enable PUC personnel to evaluate, tailor, and strengthen non-BES stakeholder cybersecurity. Non-BES stakeholders could also implement ES-C2M2 on their own, with PUCs providing oversight. To help both hire and train staff, as well as defray costs of implementing this recommendation, PUCs should take advantage of federal programs at DOE, DHS, and NIST, which are required to provide technical support. During implementation, PUCs will no doubt extract lessons learned and best practices, which should be shared with other electrical utility regulators in the state. For example, most PUCs do not oversee municipal and cooperative utilities as well as independent power producers. States may want to expand PUC purview to these stakeholders, which are small in number but growing.

- To verify the adoption of CIP standards, states should empower PUCs to hire expert staff[25] and perform on-site audits and reasonable penetration testing of non-BES stakeholders, publicly releasing their CIP compliance. Specifically, PUCs should require that a letter grade be printed on customer electrical bills or other applicable commercial invoices reflecting a non-BES stakeholder's CIP compliance, along with PUC-provided information about the benefits, risks, and costs associated with not providing electrical sector cybersecurity. An easy to understand letter grade model (i.e. A-F) for scoring utilities on their adoption of the standards will more easily incite public scrutiny, while keeping specific cybersecurity vulnerabilities ambiguous. As a majority adopts the standards, these letter grade criteria should be revised to recognize those non-BES stakeholders and their vendors that go above and beyond the PUC standards by including meaningful benefits, such as highly visible media events with state governors. This could happen gradually over time to ensure fair business treatment.

- Funding and Revenue Incentives. To help fund the adoption of PUC standards, states should provide modest matching grant funds to non-BES stakeholders to ensure technology upgrades do not become cost-prohibitive. Importantly, because standards only set minimum protections, additional resources should be made available for those non-BES stakeholders that exceed the PUC standards, along with appropriate legal protections.[26] At the same time, PUCs should be given the

[25] See the Education and Workforce section of this document.

[26] Entities that make a good faith effort to improve cybersecurity beyond the standards should be provided legal protections against possible civil penalties if doing so uncovers unknown vulnerabilities that trigger standard non-compliance. According to a Bipartisan Policy Center study, "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,

explicit authority, or encouraged to use existing authority, to provide increased ROE profit taking for non-BES stakeholders that make approved cybersecurity investments above and beyond the CIP standards. PUCs should also consider granting temporary rate increases to allow non-BES stakeholders to recoup their costs, again printing these specifics on customer bills to allow for open public debate. However, any funding provided by PUCs should require a clear, comprehensive cybersecurity plan and be subject to audit.

- *Incentives for implementation*: As critical infrastructure organizations and other private entities onboard information sharing best practices, security will improve. States should accelerate the movement towards best practices with incentives such as:
    - Requiring a minimum standard for legal protection or safe harbor provisions (guaranteed legal protection if specified standards are met);
    - Research and development funding or grants that promote competition and allocation of private funds that may not exist otherwise;
    - Providing technical assistance, particularly to smaller companies with lesser budgets and less capability;
    - Streamlining permits or security clearance approvals for employees of private entities;
    - Reducing the burden of maintaining a qualified cybersecurity workforce with access to classified information;
    - Providing tax incentives to companies that certify compliance with recognized information sharing best practices; and
    - Subsidizing cyber insurance, which can indirectly incentivize information sharing by reducing premiums for companies;

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" (Bipartisan Policy Center 2014).

CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT

States can play a major role to help fill the demand for cybersecurity careers, on both an educational and professional training level. Workforce development and education are areas where state governments are highly experienced (DoE 2012). States maintain strategic workforce plans and work to align educational institutions and training programs around the needs of regional growth sectors. These programs also provide those who are unable to afford the opportunity the ability to access and achieve a career pathway through postsecondary education and job training programs, including underrepresented demographic groups. Engaging a diverse workforce, particularly including women in cybersecurity and technology jobs is particularly important for future U.S. success, as they currently make up just 18 percent of computer science majors, and nearly half of the women who graduate with engineering degrees never enter the profession or leave soon after (Schulte 2014).

At the educational level, states can strongly influence government-supported institutions and, indirectly, private academic institutions to adopt or grow cyber education and vocational programs. Venture capital firms invested a record of $1.4 billion in 239 cybersecurity companies in 2013 (Leitersdorf and Schreiber 2014) and it is estimated that 650,000 additional cyber professionals will be needed by 2022. This growth is faster than that of all other occupations and does not include other non-technical cybersecurity jobs, such as lawyers, policymakers, intelligence analysts, linguists, and managers (BLS 2015). To excel, becoming interested in information technology at an early age is critical. Unfortunately, according to a 2014 Raytheon Survey, 82 percent of millennials say that a high school teacher or guidance counselor never mentioned to them the idea of a career in cybersecurity.

The federal government, namely DOD and DHS, offers financial incentives to universities for cybersecurity research in important industrial sectors, such as critical infrastructure, health IT, and finance. This seed funding is used to provide initial research and proof of concept for technology products in order to attract private investment. These private partners are lured by early access to research and the ability to gain favorable license terms of the technologies created. These types of programs are already having a significant impact on academic research. For example, the University of California Berkeley's (and other partner universities) Trust Center has been conducting successful research on critical infrastructure for more than ten years with funding from DOD and DHS (UCB 2005).

At the professional[27] level, there is a shortage of cybersecurity experts with an understanding of the specific challenges posed to critical infrastructure (NIST 2013b). State regulatory, information sharing, and incident response entities need expert-level

[27] For more on how cyber professionals should be defined, the authors suggest reading the latest national Research Council's report: *Professionalizing the Nation's Cybersecurity Workforce* (National Research Council 2013).

cybersecurity professionals to evaluate utility cybersecurity plans and capabilities, particularly when it comes to protecting automation and industrial control systems. Many PUCs and relevant state agencies lack these workers, and while there are free training opportunities available from the federal government and trade associations, general training does not produce cybersecurity experts. States need more highly skilled cybersecurity professionals to address the cybersecurity challenges they face (NRC 2013).

The allure of economic benefits should motivate governors and state legislators to be increasingly interested in cybersecurity workforce programs. Currently, much of the venture capital for cybersecurity businesses has coalesced in only a few states. By partnering with academia and private industry, motivated governors looking to take a piece of the growing pie can help states lead the way in developing cyber workforce and education programs.

Recommendations

- Promote cybersecurity education early. Governors and state legislators should implement policies that promote cybersecurity as a career choice and partner with institutions to support and develop cybersecurity certifications. To boost popularity, computer science and other cybersecurity-related coursework should be designated as science, technology, engineering, and mathematics (STEM) fields of study, as proposed by the National Governor's Association. STEM fields are required for graduation and would thus draw more young adults to cybersecurity fields.[28]

- Require cybersecurity in the classroom. Beginning with state schools, states should require K-12 information technology and computer programming classes, and direct post-secondary schools to offer cybersecurity classes and desirable vocational certifications. To shape the specific curricula while maintaining flexibility, governors should use their political powers to connect academia, private industry, and federal partners to develop these programs, offering incentives when necessary. At specific universities, more advanced programs built around automation and industrial control systems should be implemented, in partnership with private utilities and vendors. Furthermore, early education will breed an informed populace—increasing collective security, given that each person and their device is a potential target for cyberattack who could help spread an infection. The state of Louisiana has several cyber education initiatives that are beginning to show promise (NICERC 2017).

- Ensure electrical sector regulators have cybersecurity expertise. States should require their PUCs to certify at least one employee as a cybersecurity professional with automation and industrial control systems as well as any other applicable

[28] This recommendation was taken from the National Governor's Association document: *The Cybersecurity Workforce: States' Needs and Opportunities* (NGA 2014b).

certifications. For example, among other educational prerequisites, states could require this worker to pass the Global Industrial Cyber Security Professional (GICSP) or similar commercial equivalent. This certification is intended to "prepare enterprises, global agencies and governments to mitigate and implement a process to address ICS cyber security concerns" (GIAC 2017). States should also require all relevant agencies, including the state emergency managers, CIO and other offices, have the expert-level workforce they need. This must include a requirement for training between state responders and any entity could support a response to a cyber event in critical infrastructure.

- Governors should lead the nation in cybersecurity education and workforce development. Governors are better suited to develop customized education and vocational policies for their states by bringing together academia and private industry. Unfortunately, only a handful of governors are using the power of their office to promote cybersecurity in a meaningful way. One top executive leading the way is Governor Rick Snyder of Michigan. Using his technology background, Governor Snyder has helped to develop the nation's premier state cyber range and elevate his state's cyber workforce from multiple angles, including education, vocational programs, business support, and incident response. He has also gone so far as to create a civilian cyber militia (see Incident Response below), and Michigan also takes advantage of numerous federal funding and training opportunities (State of MI 2017). For states looking to emulate some of these best practices, the RAND Corporation published an expansive study in 2015 "Training Cyber Warriors," which should serve as a guide for training programs (Li and Daugherty 2015).

- Governors should be a catalyst for cutting-edge cybersecurity research. Much like the federal government, states could offer seed funding for cybersecurity research. Doing so would allow governors to influence research to support areas important to the state, such as the electrical sector, while partnering with private industry to keep costs to a minimum—if not making the activities profitable. Governors and agency heads would also have access to the latest research and products that would be used to protect the state's critical infrastructure. Frequent research accomplishments would beget more private industry investment in the state, strengthen the workforce, and bolster university programs.

- Work to get more women in high tech and cybersecurity fields. Women are a tremendous untapped resource for cybersecurity and high tech talent. Their low participation in high tech fields means that much of the U.S. population, of which women are more than 50 percent, is not considering the possibility of a career in cybersecurity. There are many reasons for this, including a palpable gender bias that permeates the male-dominated geek culture. Not actively engaging women in high tech and cybersecurity professions is a serious problem and opportunity cost that must be fixed. State education departments should require public school counselors, beginning in elementary school, to get young girls interested in STEM courses.

States should also partner with the various new national mentorship programs for potential female math and science majors, given that STEM education programs for kids who are selecting class electives before high school have shown to highly influence career choices and help avoid gender bias. States should take more advantage of the many federal STEM programs, particularly those with a national security flavor. For example, DOD, recognizing that the lack of STEM educated youth is a national security issue, funds the STARBASE program, many of which are operated in partnership by states. The program provides hands-on STEM education classes to fifth graders to get them excited about those career fields. Governors should engage their congressional delegation to boost matching federal funds for this program and others like it.

Additionally, diverse manpower is key to a successful cybersecurity workforce. In fact, this true not just because a diverse group almost always outperforms the best homogeneous group by a substantial margin (Page 2008), but also because a vast array of skillsets is necessary for a cybersecurity program (NIST 2013a). States must help spread the word to break stereotypes, partnering with the public and private school system to engage in directed efforts to recruit diverse groups to related STEM programs. This should include offering financial incentives and ensuring schools provide access to a mentor network. As a framework, states should draw on DHS's National Initiative for Cybersecurity Education (NICE) (NIST 2013a), using the program's National Cybersecurity Workforce Framework as a starting point, as well as the federal government's Cybersecurity National Action Plan (CNAP), which is focused on long-term strategy to strengthen cybersecurity education (Villalobos 2016).

INCIDENT RESPONSE

Despite the number of nefarious actors who have successfully exploited U.S. electrical sector networks, both federal and state cyber incident response roles, responsibilities, and capabilities are not clearly established in current plans. Federal operations are focused toward the offensive and offer vague and incomplete guidance for domestic cyber response and critical infrastructure protection, including what its responsibilities are concerning states (DHS 2013; DHS-NCCIC 2010; Bipartisan Policy Center 2014). The majority of states do not have cyber incident response plans in place and have not made clear what entity is both capable and authorized to mitigate a cyberattack, including PUCs and other electrical sector stakeholders.[29] However, states are uniquely positioned to step in and protect domestic critical infrastructure, allowing the federal government to focus on more advanced cyberattacks and international communication technology affairs.

Identifying Gaps in Coordination

Part of the problem is that there is not currently a federal agency that has been tasked with the responsibility for defending the electrical sector and there is no clear state-led solution to fill this gap (Lute and McConnell 2011; Palmer 2010; The White House 2013). DHS is charged with "coordinating" the federal effort to promote cybersecurity of critical infrastructure, and its capabilities are mainly limited to technical assistance and sharing cyber threat information (The White House 2013). Domestically, DOD is mainly charged with protecting its own networks and conducting offensive operations and does not normally operate domestically except in the event of a presidentially declared emergency, which is appropriate.[30] DOE is a participant that assists DHS in planning (Serbu 2013), but is primarily in charge of promoting baseline standards, which only affect the BES. The onus for protecting the non-BES then falls upon the States, which, as discussed previously, have the ability to affect the BES.

National incident response planning is, moreover, incomplete. According to an analysis by the Bipartisan Policy Center, an incident involving the electrical grid would be addressed through the National Cyber Incident Response Plan (NCIRP), which is designed to build on the larger U.S. National Response Framework (NRF), yet portions of the NCIRP involving states run contrary to the NRF (Bipartisan Policy Center 2014).[31]

---

[29] The authors individually called state emergency services offices and corroborated this with the National Governor's Association.

[30] According to DOD's 2015 Cyber Strategy, the three primary cyber missions of the DOD are defending its own networks, supporting military operations, and defending the U.S. homeland "if directed by the President or Secretary of Defense…to prevent destruction of property or loss of life" (DOD 2015). There are few, limited exceptions in which DOD Title 10 forces operate domestically which this paper does not describe.

[31] A report by the Bipartisan Policy Center highlights some of the many issues with the federal response plans and capabilities, including: delayed decision making; inability to create viable action plans to triage issues; unclear roles and responsibilities for state governors; inability to support requests for assistance; ambiguities in the roles and responsibilities of response agencies, including a lack of detail on the functions

Among several concerns, the two national frameworks differ on the role of governors. The NCIRP enumerates no leadership role for governors during a cyberattack, yet the NRF places governors at the center of incident response, recognizing that they are primarily responsible for protecting their population. This creates uncertainty in areas, such as the Stafford Act, where the federal government currently provides assistance to states for physical incents but may not for cyber incidents (FEMA 2013). Deficient strategic planning creates an obvious concern during an incident when federal-state bureaucratic wrangling would likely hamper decisive action and coordination efforts. States are clearly a major component of national physical disaster response, yet their role in national cybersecurity remains unclear.

Recently DHS updated its NCIRP, at the direction of PPD-41 (described below). The updated NCIRP includes strong portions, particularly the detailing of cyber Unified Coordination Groups (UCG) for significant cyber incidents and the acknowledged importance of states and critical infrastructure owner and operator participation. Additionally, the further description of DHS' incident response role in this response framework should be highly lauded, and the document's recommendation for state cyber incident response plans is a strong one with thorough guidance. However, the updated NCIRP seems to still be limited when describing the roles of states to information sharing platitudes and boilerplate language touting the "importance" of "working closely" to coordinate and share information. There are hardly any details for integrating states in the NCIRP and UCG beyond these loose terms throughout the documents, as well as in the description of the UCG construct for asset response, which is DHS' role, and the annex describing Core Capabilities and Critical Tasks (DHS 2016b). In fact, the updated NCIRP conspicuously notes that states "are responsible for ensuring preparedness, response, and recovery activities within their jurisdiction" (DHS 2016b).

States have an opportunity to take a leadership role in critical infrastructure protection and we have heard from many states that they want to actively engage critical infrastructure operators, especially because the federal government "…typically will not play a role in this line of effort…" (DHS 2016b).[32] It is critical to describe the roles and responsibilities and specific ways how states will participate in national cyber response. Unfortunately, the updated NCIRP falls short, and DHS is not going to come riding in on a white horse to save the day—it does not have the capabilities nor the legal responsibility to do so, beyond acting as an information sharing and coordinating entity.

---

of response organizations; and uncertainties over the statuary authority for federal assistance, including how the Stafford Act may allow federal support and reimbursement to states. 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 (BPC 2014). The NCIRP relies on separate mechanisms to coordinate cyber-response efforts, including the NCCIC and the Cyber Unified Coordination Group's Incident Management Team.

[32] "When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity." (DHS 2016b).

Recent White House Action – Presidential Policy Directive 41

On July 26, 2016, the White House released PPD-41, United States Cyber Incident Coordination. The directive rightly diagnoses that current policies may not adequately address "significant cyber incidents" and that all levels of government have a role and responsibility in protecting the nation from malicious cyber incidents. PPD-41 even acknowledges that states "have responsibilities, authorities, capabilities, and resources" and should be a partner with federal response. However, the directive stops short of providing policies for how states will be involved in incident response.

For our purposes of electrical sector cyber incident response, the directive is predominantly a reiteration and codification of current policy and, in its own words, "is intended to result in unity of effort and not to alter [federal] agency authorities." PPD-41 focuses on "Significant Cyber Incidents" and makes clear that the White House will be the center of national cyber incident response policy and strategy. This seems to be the primary focus of the directive. Specifically, PPD-41 identifies the White House's Cyber Response Group (CRG), run by the Assistant to the President for Homeland Security and Counterterrorism, as the policy and strategy hub. However, states are virtually omitted from the White House's cyber incident response coordination document. At a strategic level, PPD-41 goes through a vastly comprehensive list of federal agencies that will participate in national response policy and strategy making but patently leaves the states entirely. At the tactical level, PPD-41's more detailed Annex describes does not address how states should be involved in national response, except to reiterate "coordination."

Additionally, it is important to note that PPD-41 largely avoids changing federal policies with respect to the private sector. This is particularly conspicuous as most critical infrastructure is not government-owned. The directive states that "when a cyber incident affects a private entity, the federal government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity."

State Government Response

State governments are slowly realizing that they play an important role in protecting critical infrastructure. Unfortunately, throughout the course of research for this paper, it was clear that most states have not designed cyber incident response plans—and for those that have, their capability and capacity to thwart cyberattacks are minimal. This is a far cry from their leadership roles in planning for, and responding to, physical emergencies where states possess much of the nation's capability and capacity. Without clear responsibilities and capabilities for domestic cybersecurity, a government-wide incident response gap exists. Importantly, state response planning suffers from the same shortcoming as federal response plans: They do not properly incorporate the private

sector, including critical infrastructure operators, into the emergency response operations (Rogers 2015).[33]

Fortunately, several state governors have bucked this trend by directing the development of a comprehensive incident response plan and cyber capability to mitigate attacks. Again, Michigan has been a leader: Governor Rick Snyder has created the Michigan Cyber Initiative, a forward-looking initiative that is the umbrella for the state's many cybersecurity programs, including its cyber incident response plan, incident response capabilities, education and workforce initiatives, cyber training range, public awareness campaigns, and outreach to the federal government. Michigan also created a centralized security department run by a chief security officer who brings together both physical security and cybersecurity—analogous to this paper's Cybersecurity Coordinator recommendation—and the Cyber Civilian Corps to assist in response to emergencies, much like volunteer fire departments.

Response Capabilities

One challenge states have had with incident response is growing their cybersecurity capabilities. State emergency management agencies for the most part have jurisdiction over all state emergency response, including cyber. This is important because cybersecurity is not an IT issue but a whole of government issue. Unfortunately, as mentioned above, most state governors have access to little cyber capability and employ few cyber professionals (as opposed to their capabilities during physical disasters). State emergency management agencies often call upon the National Guard[34] as a force provider during state emergencies, using everything from large assets like state-of-the-art C-130 firefighting aircraft to special operations search and rescue units to counter-drug intelligence analysts. Federal agencies also draw on the National Guard, via the Defense Support to Civil Authorities authority, to assist in domestic operations. For instance, the Coast Guard often calls on their search and rescue capabilities to rescue stranded seafarers, and could do so to support their port cybersecurity mission as well. Unfortunately, despite clear domestic needs, DOD is still in the process of creating clear policies and mission requirements for National Guard cybersecurity activities—a prerequisite for National Guard units to be created and therefore afforded to governors. State emergency management agencies are far smaller than their state National Guard counterpart and the lack of access to cyber capabilities and funding – compared to that available for physical operations – is significantly limiting.

[33] According to CYBERCOM Commander Admiral Michael Rogers, there is no current "legal and policy framework" for sharing the Defense Department's cybersecurity capabilities with the private sector (Rogers 2015).

[34] It is important to remember that state National Guards are a supporting agency, directed by the governor; they assist in the operations of other governmental agencies, or the private sector, and do not act coercively or autonomously.

National Guard and Domestic Cybersecurity

Compared to National Guard physical emergency response, there is little participation from these forces in domestic cyber incident responses; their use is complicated by a variety of bureaucratic issues and an unwillingness to develop policies to use the National Guard nationally. In a 2016 report, the Government Accountability Office echoed this concern, recommending that DOD clarify roles and responsibilities for the National Guard during domestic cyber incidents, particularly when acting in support of other federal agencies (GAO 2016). The authorities for this support already exist in the physical domain but have not been freed from ambiguity when applied to cybersecurity activity. Because National Guards are the combat reserve to the active duty military, they largely mirror the active duty Army and Air Force, are federally resourced and are trained to a high proficiency; yet, they reside under the control of the governor when not deployed. This allows National Guards to be uniquely positioned for use in domestic emergencies, including cybersecurity (Goure 2016).

Employing the National Guard provides several advantages. Most National Guard forces are part-time military members, working full-time in the private sector, and in many instances in the very industry the National Guard supports, such as first responders, electrical utilities companies, communication and technology industries. National Guard members who work in Silicon Valley bring cutting-edge skills, experience, and knowledge, which could yield immediate benefit to the defense of the electrical sector. Guardsmen working full-time in the cyber industry are exposed to a much larger portion of the cyber domain than their active duty counterparts, which complements their military training. This is particularly relevant in the cybersecurity industry where knowledge and skills are highly perishable, and where adversaries develop and employ new techniques at an incomparably accelerated pace. In addition, National Guardsmen, while acting in non-federal duty status, provide flexibility to conduct missions that active duty forces cannot. This includes in the context of law enforcement missions due to the *Posse Comitatus Act*, which specifically prohibits federal military forces from supporting law enforcement activities—an important distinction, as many cyber incidents in the homeland are cybercrimes.

The National Guard could also provide a solution for attracting cyber talent to government cybersecurity efforts to build the future cyber workforce necessary. Recruiting and retaining highly skilled cyber personnel is not just a state-level problem, but also one of the greatest challenges facing both the military and DHS (Pellerin 2013). The Defense Science Board has identified a “burnout factor” among elite government cyber professionals, stating, “It is not clear that high-end cyber practitioners can be found in sufficient numbers” (Johnson 2012; Defense Science Board 2013). Meanwhile, DHS’s double-digit vacancy rate for top cybersecurity jobs continues. The private sector and competitive hiring by the intelligence community beckon cyber professionals with large paychecks, less commitment, and a better quality of life. Increased cyberattacks and cyber espionage have spawned a massive industry need for cyber specialists that is poaching the best talent from the federal government (Anderson 2013). This demand is

set to grow 22 percent in the next decade, with salaries rising five to seven percent per year (Apps and Goh 2013). The National Guard is inherently resistant to recruitment and retainment issues because it offers professionals many of the benefits of military or government service with little career and lifestyle sacrifice. As the private cybersecurity industry grows, so does the eligible talent for National Guard recruitment. Cybersecurity capability is about people, and garnering top talent is paramount (DoD 2011, 2015) as innovative hacking techniques continue to proliferate regardless of how well networks can defense themselves (Kaplan 2013). Unfortunately, as of now, National Guard cybersecurity units are few in number.[35]

For the most part, DOD has been reluctant to provide requirements or resources for the National Guard, which means their role in the cyber domain is relatively ambiguous and governors do not know what precisely they are allowed or not allowed to do. For governors, sorting out such ambiguities has been frustrating. Moreover, existing defense strategies for the integration of the National Guard into cyber operations are limited to load sharing and surge capacity for the active duty forces and for protecting internal National Guard networks—a relatively limited responsibility. According to DOD's recent "most comprehensive study to date of the Reserve Component," the National Guard's function will be limited to supporting roles coordinating, training, advising, and assisting, rather than an operational role to actually stop a cyberattack (DoD 2014). The Government Accountability Office recently said of the National Guard's participation in cybersecurity incidents, "[DOD] documents do not identify the role of the dual-status commander—that is, the commander who has authority over federal military and National Guard forces—in supporting civil authorities during a cyber incident. According to U.S. Northern Command officials, in a recent cyber exercise there was a lack of unity of effort among the DOD and National Guard forces that were responding to the emergency but were not under the control of the dual-status commander" (GAO 2016). In addition, there is no plan or initiative for DHS to use the National Guard in national domestic cyber operations, as they do in a very significant way for national physical incidents. Other federal agencies are beginning to recognize and utilize the National Guard; just as the FBI has entered into a legal memorandum of agreement with the California National Guard to help solve cybercrimes, so could the DHS enjoy an expanded National Guard relationship.

Interestingly, in DHS' recently revised National Cyber Incident Response Plan for 2017, the Department asserts that National Guard units may act unilaterally in a State Active Duty status or as a supporting force provider for a federal entity in Title 32 status, perform cyber incident response, saying, "At the direction of a State Governor and Adjutant General, the National Guard may perform state missions, including supporting civil authorities in response to a cyber incident" (DHS 2016b). However, there are three

[35] To its credit, U.S. CYBERCOM is beginning to discuss increasing the use of state National Guards and the National Guard Bureau recently announced the beddown of ten-eleven small 32 person "Cyber Protection Teams," but this will take five or so years and Army CYBERCOM Commander General Edward Cardon has said DOD may limit their authorities to protecting National Guard networks. (DOD 2014)

currently prohibitive policy issues. First, DOD has not provided the authorities of the National Guard operating in a federal Title 32 status, under the control of the governor, beyond what is considered a limited mission of protecting internal networks and training, advising and assisting. Moreover, "supporting civil authorities" (aka Defense Support of Civil Authorities, DSCA) is something that Governors cannot direct and must be requested by the supporting agency and approved by DOD.

Second, DOD has not authorized governors or adjunct generals to utilize their National Guard unilaterally during a cyber incident. DOD has not, despite requests from states, provided operational guidance and regulatory policy on what states can and can't do with their National Guard in a State Active Duty status; in fact, it has purposely limited the authorities of the National Guard in both this status and Title 32 statuses.[36]

Lastly, according to several state governors' offices interviewed, DOD has asserted that it will limit the "information, software, hardware, systems, tools, tactics, techniques, and procedures" National Guardsmen may employ in performing domestic cybersecurity actions on behalf of a Governor if DOD considers them classified—an unnecessary, unenforceable and arduous restriction.[37] This policy would categorically obstruct the National Guard's ability to conduct cybersecurity operations domestically. It is impossible to enforce at scale, and likely hinders the federal government's goal of protecting critical infrastructure. Why not share classified information with the National Guard as DHS does with private sector stakeholders? Who would decide what technique or software, for example, is classified? How would they keep up with the scale of this endeavor and the millions, if not trillions, of new pieces of software code related to cybersecurity and the tactics and techniques that are constantly emerging? Would classification of these also be attributed to those used or made in the private sector? It is likely that the private sector has more advanced procedures, software, and tactics for dealing with cyberattack than much of the DOD, so would they too be subject to DOD approval? If not, why wouldn't the private sector be subject to these limitations, but fully vetted National Guardsmen would be? If so, this would be extremely problematic and would likely cause Silicon Valley to erupt in protest to DOD and the Congress. In addition, shouldn't National Guard and Reserve personnel share best practices they learn from their private sector job and bring them to the DOD for their use? And if they are unable to act upon classified intelligence, information sharing is rendered far less effective—a curious limitation as DHS provides classified information to states and private actors, as discussed above. Finally, and most importantly, the classification limitation could result in loss of property or even lives. If a guardsman had the capability to thwart or discover a cyber threat but was limited by the tactics they could use, or even the approval process to use those tactics, they would not be allowed to mitigate the

[36] This information was researched via off the record discussion with several state governors' offices, the NGA and the Secretary of Defense's office throughout 2016, including viewing official documents describing these limitations.

[37] This information was researched via off the record discussion with several state governors' offices and the Secretary of Defense's office in April, 2016.

attack. In other words, personnel could have the capability to stop a cyber attack but might be prevented from doing so by regulation.

Recommendations

- Governors should lead the way in domestic cybersecurity response, allowing the federal electrical sector regulators to focus more on advanced threats. Governors are ultimately responsible for protecting their populations. Unfortunately, a significant gap exists between the recognized roles and responsibilities of federal agencies[38] and those undertaken by states in protecting the electrical sector. The lack of planning and capability building by states to prepare for and respond to cyberattacks mean that states either expect that the federal government will ultimately take responsibility for helping to protect the electrical sector or that they are not vulnerable to attack. Each conclusion is misguided; states, led by governors, should be at the forefront, and embolden themselves to help protect the electrical sector.

  Governors should begin by assessing risk and developing a master cybersecurity incident response plan. Constructing a risk assessment is key to operational planning; only after governors have assessed their risk of cyber incident can they adequately detail what level of capability they need and what support they would require from the federal government during a catastrophic incident. Governors should know the threat landscape and risk tolerance for the state, agencies, and electrical sector infrastructure. Once the assessment is complete, governors should develop master incident response plans to combat threats and determine what investments must be made. Incident response plans should define who is in charge, what capabilities they have and need, what each stakeholder's roles and responsibilities are, and how coordination with federal government and private industry will work. To accomplish this, governors should immediately stand up a cyber incident response taskforce to put these plans together or review current plans if one exists. It is important that these efforts be governor-led, in coordination with state Cybersecurity Coordinators, to ensure their importance and a whole-of-government approach. Plans should also detail how the state coordinates with non-BES stakeholders and private industry as well as law enforcement regarding criminal investigations, similar to how physical emergency efforts are conducted.

  To assist in these actions, several federal resources exist for governors to take advantage of, most predominantly, the National Institute for Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure*

[38] Federal agencies of jurisdiction in the electrical sector are the Department of Energy, North American Electric Reliability Corporation, Federal Energy Regulatory Commission, and Department of Homeland Security.

Cybersecurity. Leveraging available technical assistance from DHS, states can use the framework to help define their cybersecurity posture, develop risk profiles, estimate workforce and education needs, calculate costs to mitigate intolerable risk, and install response capabilities appropriate for their level of risk. All state governors should apply the NIST Framework and participate in the DOE's ES-C2M2 to assess, tailor, and strengthen their cybersecurity capabilities.

To their credit, state executives are beginning to get serious in developing cybersecurity policies for their states. The National Governors Association (NGA) has been at the center of this promotion. In 2013, for the first time, the NGA made cybersecurity one of its primary meeting agenda items at the annual meeting of all state governors, following several high-profile attacks on state government.[39] The NGA also issued a "Call to Action," identifying the key cybersecurity issue areas and providing a framework to begin state cybersecurity planning efforts (NGA 2013). Governors should build on the recommendations of the NGA by establishing large interstate cyber exercises, to complement the many national cyber events. States with large cyber range capacity, such as Michigan, could host these events for little cost, and federal agencies and electrical industry partners should also participate.

One cause for the dearth of state planning efforts may be a lack of federal dollars or incentives, particularly for small states. DHS offers grant funding for state cybersecurity, but these grants are highly limited and often compete for the same dollars as FEMA non-disaster preparedness grants. DHS should offer separate incentives or grants for cybersecurity planning, similar to DOD's defense planning funding through the Office of Economic Adjustment, in addition to the technical assistance they and the NIST offer.

- States and governors should be directly involved in national cyber incident response efforts and policy making. DHS should update federal disaster response frameworks, such as the NCIRP and NRF, and clarify both federal and state roles and responsibilities, as well as identify opportunities for entrepreneurial governors to go above and beyond what is required of them. Platitudes describing the importance of information sharing and working together are not enough. Further, the recent PPD-41 codifies the White House's Cyber Response Group as the authority of national cyber incident response policy and strategy but both misses the opportunity to include states and governors in any meaningful role and did not make any significant changes in the updated NCIRP. To rectify this, the CRG

[39] In October 2012 the U.S. Secret Service notified the State of South Carolina that residents' private information had been stolen from state networks (Isikoff 2012). The investigation revealed a more than one-month-long cyber intrusion into the SC tax system, resulting in the exposure of 3.6 million social security numbers (McLeod, Jenkins, and Barbara 2012) and 1.6 million income tax returns (Raduege 2013). Apart from intangible costs such as loss to reputation and credibility, that breach is estimated to cost approximately $20 million.

membership should be amended to include the Council of Governors, who would represent states on this important policy committee.

In addition, electrical sector stakeholders should work to increase participation in cyber incident response exercises, as many states do not participate regularly. The federal government should aggressively incentivize all states to participate, including by withholding certain federal funds for those who decline.

- Governors should take further advantage of DHS cyber programs. There are many federal resources available to states that, according to DHS, are underutilized (DHS 2014). One of these is DHS's *Cyber Resilience Review* (CRR). The CRR is a no-cost program provided to states that assesses their operational resilience and ability to manage cyber risk, including to critical infrastructure. The CRR provides governors with a clear report summarizing cross-agency strengths and weaknesses, and recommends improvements to the state's cyber incident risk posture and state preparedness plans. Discussions with DHS revealed a severe lack of interest in the CRR from state leaders.

- The National Guard should be fully resourced, equally trained, equipped and authorized to use all available tactics, and made a key part of domestic cyber incident response. When it comes to domestic critical infrastructure protection, DHS's role has been one more of enablement through information sharing than strict oversight, and governors should realize that they will be held responsible in the event of a significant cyber incident on the electrical sector. While it is true that electrical sector stakeholders have the responsibility to protect their own networks from cyberattack (DHS 2013a; The White House 2013), electricity is a public good and governors should have all the tools in the toolbox at their disposal, particularly if the severity of a cyber incident escalates above the capabilities of the electrical sector entity (just as in the case of a physical emergency). To this end, the restriction on using "software, hardware, systems, tools, tactics, techniques, and procedures" that the DOD considers classified must be removed and replaced with a workable solution, such as a specific restriction on using intelligence information that is deemed classified without the DOD's consent. The current policy could very well mean unnecessary loss of life or property.

  States, not the federal government, hold much of the capability to respond to natural disasters, and should build similar capabilities for cyber incident response. States should designate emergency management agencies as the state's cyber incident response entity, using the National Guards as a primary force provider and in coordination with the above-recommended state Cybersecurity Coordinators. Housing cyber incident response in state emergency management agencies is key to mitigating cyber incidents as cybersecurity is not merely an IT

issue and must encapsulate a whole-of-government approach.[40] The federal government recognized this when the President declared DHS in charge of coordinating domestic critical infrastructure protection (The White House 2013, 2013). In addition, state emergency management agencies have extensive experience working within the existing National Response Framework—directing the National Guard and requesting FEMA support for physical disasters—which could be easily transferred to cyber incidents. This will have the added effect of better mitigating cyberattacks that coincide with physical incidents, whether nefarious or natural. This process is in its nascent stages, but only in a handful of states (Goure 2016).

Finally, governors should aggressively advocate that the National Guard be properly resourced to DOD and DHS, as well as to their congressional delegations, to provide the necessary cybersecurity capabilities for critical infrastructure protection. This would begin with DOD creating military requirements for cybersecurity operations, which may require congressional action to provide explicit authorization for National Guard cybersecurity activities in Title 32 of the U.S. Code (Goure 2016). Key to the success of the National Guard is access to the same skillset, training, and mission opportunities as the active component military, which will boost recruitment and retention within DOD, as the National Guard is relatively unaffected by the nationwide shortage of cybersecurity professionals. Building on this advantage, the National Guard Bureau should implement training standards that exceed military requirements that are geared specifically toward critical infrastructure protection.[41] Generating cybersecurity requirements for the National Guard will require adding force structure and end strength numbers to the National Guard, to avoid gutting the current National Guard units, which are already set to shrink in the coming years. It is important to realize that this is not an exclusive benefit for state government: The federal government, particularly DOD, would benefit greatly from its rapid access to highly capable National Guard cybersecurity units, when needed for federal missions.

[40] For those states that choose not to do this, the authors highly recommend defining who is in charge of state cybersecurity and if this responsibility is shared in any way those lines of responsibility should be clearly enumerated.

[41] Though active military cyber training and standards are rigorous, they are not enough. In addition to earning a baseline Military Occupational Specialty/Air Force Specialty Code qualification from an accredited Service component school or institution, members should also meet DODI 8570.01-M, *Information Assurance Workforce Improvement Program*, established by the Assistant Secretary of Defense for Networks and Information Integration, and the DOD Chief Information Officer. Guard personnel in cyber formations should for example also hold commercially recognized certifications, like CompTIA Security +, ISC2 CISSP, EC C|EH, Cisco CCNA/CCNP, SANS GSEC and GCIH, SCADA related certifications and participate in one national cyber exercise annually.

CONCLUSION

State and local agencies ensure much of electrical grid reliability. Unfortunately, few resources have been committed for cybersecurity activities, especially given the potential consequences. Dozens of official government and independent reports have yielded numerous insightful policy recommendations imperative to electrical grid reliability, yet they rarely address the non-BES, states and other stakeholders, or its importance. A dearth of accessible information and understanding of the non-BES, lack of funding, and misplaced priorities by senior leaders have therefore limited non-BES cybersecurity. Serious gaps exist in electrical sector cybersecurity, state government cybersecurity, cybersecurity information sharing, private sector and state cooperation, establishing standards, cybersecurity education and workforce development, and incident response. By unpacking the critical role states play across these six topic areas of domestic cybersecurity, policymakers can begin to fill these voids.

The implementation of technology that facilitates information sharing is essential to pushing both private and public sector cybersecurity operations toward adoption of best practices. In this case, information sharing depends upon the ability to communicate rapidly and reliably, so the automation and adoption of a common language are essential. States need to take advantage of resources offered by entities like DHS and leverage their own budgets to capitalize on opportunities to make targeted investments. States should work with private owners and operators to implement standardized information sharing protocols, such as STIX/TAXII and CRISP, into their critical infrastructure sectors. States must also take a proactive approach to procurement of security-minded technology, building security services into contracts and reducing the exposure of the state to cybersecurity risks.

This paper is a stepping-stone towards a joint state, federal, and private sector cyber resiliency plan for the total electrical grid, including the BES and non-BES. The only way to establish a truly robust cyber resiliency program is by addressing all of the different stakeholders and elements of the problem at the same time. We must have a comprehensive solution that is inclusive of the private sector as well as local, federal, and state governments, and thus every party must play its part. Again, as Ted Koppel writes, “American democracy rests on a foundation of competing tensions among local, state, and federal laws, and laws governing the electric power industry reflect those tensions” (Koppel 2015). This paper aims to provide just one piece of that puzzle.

Works Cited

Alden, William. 2013. “Computer Bugs and Squirrels: A History of Nasdaq’s Woes.” *DealBook*. August 22. http://dealbook.nytimes.com/2013/08/22/computer-bugs-and-squirrels-a-history-of-nasdaqs-woes/.

Anderson, Sharon. 2013. “CHIPS Articles: Recruiting, Training and Maintaining Talent in the Cyber Workforce.” July. http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4727.

Apps, Peter, and Brenda Goh. 2013. “Cyber Warrior Shortage Hits Anti-Hacker Fightback.” *Chicagotribune.com*. Accessed October 19. http://www.chicagotribune.com/business/sns-rt-us-security-internet-20131013,0,6022548.story.

Ashton Carter. 2013. “Defense.gov Transcript: Remarks by Deputy Secretary of Defense Carter at the Aspen Security Forum at Aspen, Colorado.” *Remarks by Deputy Secretary of Defense Carter at the Aspen Security Forum at Aspen, Colorado*. July 18. http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5277.

Bipartisan Policy Center. 2014. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat.” http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

Cynthia Bogorad and Latif Nurani “NERC’S Definition of The Bulk Electric System” Why The Definition Matters, Why It’s Changing, And Where We Stand At NERC And FERC.” Spiegel & Mcdiarmid LLP. http://www.spiegelmcd.com/files/APPA_Legal_Seminar_Paper_NERC_BES_2012_10_25_09_08_51.pdf.

Campbell, Richard J. 2015. “Cybersecurity Issues for the Bulk Power System.” Congressional Research Service. https://www.fas.org/sgp/crs/misc/R43989.pdf.

Comey, James. 2016. “FBI Director Warns of ‘Terrorist Diaspora’ after Islamic State Crushed.” *UPI*. September 27. http://www.upi.com/Top_News/US/2016/09/27/FBI-director-warns-of-terrorist-diaspora-after-Islamic-State-crushed/6791474995369/.

Defense Science Board. 2013. “Resilient Military Systems and the Advanced Cyber Threat.” DEFENSE SCIENCE BOARD WASHINGTON DC, DEFENSE SCIENCE BOARD WASHINGTON DC. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

DHS. 2013. “National Response Framework.” DHS. http://www.fema.gov/media-library/assets/documents/32230?id=7371.

———. 2014. States Underutilize DHS Resources, According to Confidential DHS Source.

———. 2015. “FEMA Non-Disaster Preparedness Grants.” http://www.fema.gov/preparedness-non-disaster-grants.

———. 2013a. “Cybersecurity Is Everyone’s Business.” *DHS: Cybersecurity Is Everyone’s Business*. Accessed October 15. http://www.dhs.gov/cybersecurity-everyones-business.

———. 2013b. “Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD 21 Critical Infrastructure Security and Resilience.” *EO 13636 Fact Sheet*. Accessed October 5. http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.
DHS. 2016. “Revised National Cyber Incident Response Plan (NCIRP) 2016.” *The National Cyber Incident Response Plan*. December. https://www.us-cert.gov/ncirp.
DHS-NCCIC. 2010. “National Cyber Incident Response Plan.” Department of Homeland Security. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.
DoD. 2011. “DoD Strategy for Operating in Cyberspace July 2011.” http://www.defense.gov/news/d20110714cyber.pdf.
———. 2014. “Cyber Mission Analysis: Mission Analysis for Cyber Operations of the Department of Defense.” DoD. http://www.ngaus.org/sites/default/files/pdf/DODCYBER%20FY14%20NDAA%20Sec%20933%20REPORT%20FINAL.pdf.
———. 2015. “The Department of Defense Cyber Strategy.” DoD. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
DoE. 2012. “Federal Role in Education.” Websites. *Federal Role in Education*. February 13. http://www2.ed.gov/about/overview/fed/role.html.
DOE. 2013. “National Response Framework - Emergency Support Function #12 – Energy Annex.” Department of Energy. http://energy.gov/oe/services/energy-assurance/response-and-restoration/esf-12-events.
———. 2014. “State Energy Program.” http://energy.gov/eere/wipo/about-state-energy-program.
Edison Electric Institute. 2015. “Frequently Asked Questions About Cybersecurity And The Electric Power Industry.” October. http://www.eei.org/issuesandpolicy/cybersecurity/documents/cybersecurity_faq.pdf.
EEI. 2014. “Electric Power Industry Initiatives to Protect The Nation’s Grid From Cyber Threats.” Edison Electric Institute. http://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Cybersecurity%20Backgrounder.pdf.
FERC. 2010. “An Overview of the Federal Energy Regulatory Commission and Federal Regulation of Public Utilities in the United States.” http://www.ferc.gov/about/ferc-does/ferc101.pdf.
———. 2014. “What FERC Does.” *FERC: About FERC*. June 24. http://www.ferc.gov/about/ferc-does.asp.
FERC and NERC. 2012. “Arizona-Southern California Outages on September 8, 2011.” FERC and NERC. http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

FireEye. 2014. “White-Paper-Security-Reimagined-An-Adaptive-Approach-to-Cyber-Threats.pdf.” http://webobjects.cdw.com/webobjects/media/pdf/FireEye/White-Paper-Security-Reimagined-An-Adaptive-Approach-to-Cyber-Threats.pdf.

Fleming, Matthew H., and Eric Goldstein. 2011. “An Analysis of the Primary Authorities Governing and Supporting the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States.” HSI Report. Arlington, VA: HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE. http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf.

GAO. 2015. “Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning.” Government Accountability Office. http://www.gao.gov/products/GAO-15-749.

———. 2016. “Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents.” April 4. http://www.gao.gov/products/GAO-16-332.

Global Advisory Committee. 2015. “Integration for Fusion Centers - An Apendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers.” file:///Users/andreasmueller/Downloads/Cyber%20Integration%20for%20Fusion%20Centers.pdf.

Goure, Daniel. 2016. “National Guard and The U.S. Power Grid | RealClearDefense.” July 11. http://www.realcleardefense.com/articles/2016/07/11/national_guard_and_the_us_power_grid_109548.html.

Grady, Mark, and Francesco Parisi. 2011. *The Law of Economics of Cybersecurity*. http://www.cambridge.org/us/academic/subjects/law/law-general-interest/law-and-economics-cybersecurity.

Hayden, Michael. 2014. *Cybersecurity and the North American Electric Grid Panel Discussion*. Bipartisan Policy Center. http://bipartisanpolicy.org/library/cybersecurity-electric-grid/.

———. 2014. “Electric Grid Cybersecurity: Michael Hayden & Industry Perspectives.” *C-SPAN.org*. Accessed November 6. http://www.c-span.org/video/?314419-1/electric-grid-cybersecurity-michael-hayden-industry-perspectives.

ICS-CERT. 12-15. “FY2015 ICS-CERT Report.” *ICS-CERT Monitor for FY2015*. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf.

ICS-CERT. 2015. “May-June 2015 | ICS-CERT.” *ICS-CERT Monitor June 2015*. July 7. https://ics-cert.us-cert.gov/monitors/ICS-MM201506.

ICS-CERT. 2016. “Overview of Cyber Vulnerabilities | ICS-CERT.” https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities.

Isikoff, Michael. 2012. “One Email Exposes Millions of People to Data Theft in South Carolina Cyberattack.” *NBC News*. November 20. http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack.

Johnson, Nicole. 2012. “DHS to Hire 600 Cyber Professionals – Fedline - The Federal Times Blog - Federal News, Government Operations, Agency Management, Pay & Benefits.” *Fedline*. October 31. http://blogs.federaltimes.com/federal-times-blog/2012/10/31/dhs-to-hire-600-cyber-professionals/.

Kaplan, Jay. 2013. “CYBER7: The Seven Key Questions Driving the Cybersecurity Agenda - POLITICO.com.” Expert Panel presented at the Cyber7, The Newseum, Put on by Politico, October 8. http://www.politico.com/events/cyber-7-the-seven-key-questions/.

Keogh, Miles, and Christina Cody. 2012. “Cybersecurity for State Regulators.” http://energy.gov/oe/articles/naruc-releases-cybersecurity-primer-utility-regulators-june-2012.

Kevin Mandia. 2015. “Data Breach a Warning for States.” *Sacbee*. June 16. http://www.sacbee.com/news/politics-government/the-state-worker/article24667198.html.

Koppel, Ted. 2015. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. 1st edition. New York: Crown.

Leitersdorf, Yoav, and Ofer Schreiber. 2014. “Is a Cybersecurity Bubble Brewing? Information Security Technologies Data Breaches - Fortune.” *Is a Cybersecurity Bubble Brewing?* July 17. http://fortune.com/2014/06/17/is-a-cybersecurity-bubble-brewing/.

Li, Jennifer J., and Lindsay Daugherty. 2015. “Training Cyber Warriors.” Product Page. http://www.rand.org/pubs/research_reports/RR476.html.

Lipman, Paul. 2015. “4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective).” July. http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html.

Longstaff, Tom. 2015. “Vulerabilities - Scada Systems? | Cyber War! | FRONTLINE | PBS.” http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/scada.html.

Louisiana Tech University. 2016. “Cyber Innovation Center & Louisiana Tech University.” *Cyber Innovation Center & Louisiana Tech University Launch Cyber Education Program for Nation’s K-12 Educators*. http://nicerc.org/2016/04/cyber-innovation-center-louisiana-tech-university-launch-cyber-education-program-for-nations-k-12-educators/.

Lute, Jane Holl, and Bruce McConnell. 2011. “Op-Ed: A Civil Perspective on Cybersecurity | Threat Level | Wired.com.” *Wired*. February 14. http://www.wired.com/threatlevel/2011/02/dhs-op-ed/.

McDonald, T. S. 2012. *The Smart Grid Imperative: Five Powerful Factors Energizing Utilities Today*. S.l.: T.S. McDonald Associates.

McGuinness, Meghan. 2014. “A New Organization for Cybersecurity across the Electric Grid.” *Bulletin of the Atomic Scientists*. Accessed November 6. http://thebulletin.org/new-organization-cybersecurity-across-electric-grid7046.

McLeod, Harriet, Colleen Jenkins, and Philip Barbara. 2012. “Taxpayer Data Exposed in Cyber Attack on South Carolina Agency.” *Reuters*, October 26.

http://www.reuters.com/article/2012/10/26/us-usa-cybersecurity-southcarolina-idUSBRE89P16E20121026.
Miller, Greg. 2013. “FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered - The Washington Post.” News Article. November 14. https://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.
NARUC. 2014. States Willfully Ignorant of Possible Cybersecurity Challenges in the Electrical Sector.
———. 2017. “NARUC Releases Updated Cybersecurity Manual.” *NARUC*. January. https://www.naruc.org/about-naruc/press-releases/naruc-releases-updated-cybersecurity-manual/.
NASCIO & Deloitte. 2012. “State Governments at Risk: A Call for Collaboration and Compliance.” NASCIO & Deloitte. www.nascio.org/.../Deloitte-NASCIOCybersecurityStudy2012.pdf.
NASCIO. 2014. “State Governments at Risk: Time to Move Forward.” NASCIO & Deloitte. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf.
NASEO. 2015. Interview with NASEO officials and an confidential state energy official.
NERC. 2014. “APS, FERC and NERC Reach Settlement Agreement on September 2011 Southwest Blackout,” July 7. http://www.nerc.com/news/Headlines%20DL/APS%2007JUL14.pdf.
———. 2015. “Glossary of Terms Used in NERC Reliability Standards.” NERC. http://www.nerc.com/files/glossary_of_terms.pdf.
New Jersey Board of Public Utilities. 2016. “Christie Administration Adopts Comprehensive Cybersecurity Requirements for Regulated Utilities.” New Jersey Board of Public Utilities. http://nj.gov/bpu/newsroom/announcements/pdf/20160318OHSP_pr.pdf.
NGA. 2013. “Act and Adjust: A Call to Action for Governors for Cybersecurity.” NGA. http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf.
———. 2014a. “NGA: OVERVIEW OF STATE HOMELAND SECURITY GOVERNANCE STRUCTURES.” http://www.nga.org/files/live/sites/NGA/files/pdf/2014/HomelandStateGovernanceStructures.pdf.
———. 2014b. “Cybersecurity Workforce Key To Combating Threats.” *Cybersecurity Workforce Key to Combating Threats*. October 27. http://www.nga.org/cms/home/news-room/news-releases/2014--news-releases/col2-content/cybersecurity-workforce-key-to-c.html.
Page, Scott E. 2008. *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies*. New edition with a New preface by the author edition. Princeton: Princeton University Press.
Palmer, Adam. 2010. “Cyber Security: The Road to Security Begins with Personal Responsibility | Symantec Connect Community.” *Symantec*. June 1.

http://www.symantec.com/connect/blogs/cyber-security-road-security-begins-personal-responsibility.
Pellerin, Cheryl. 2013. “Defense.gov News Article: Critical Cyber Needs Include People, Partners, General Says.” *DoD*, July 2. http://www.defense.gov/news/newsarticle.aspx?id=120402.
Peter Behr, and Blake Sobczak. 2015. “SECURITY: States Search for Strong Cyberdefense Strategies.” *States Search for Strong Cyberdefense Strategies*. February 17. http://www.eenews.net/stories/1060013552.
PUC Official. 2-16 & 1-17. PUC Interview Phone Call.
Raduege, Harry. 2009. “Cyber Security and the States | CivSource.” Interview. *CivSource*. October 5. http://civsourceonline.com/2009/10/05/cyber-security-and-the-states/.
———. 2013. Lecture. Lecture, July.
Rogers, Michael. 2015. “Military Cybersecurity Hearing Discusses Cyber Threats, Information Sharing | Inside Privacy.” *Military Cybersecurity Hearing Discusses Cyber Threats, Information Sharing*. March 6. http://www.insideprivacy.com/united-states/congress/military-cybersecurity-hearing-discusses-cyber-threats-information-sharing/.
Stempfly, Roberta. 2013. *Cyber Incident Response: Bridging the Gap between Cybersecurity and Emergency Management*. House of Representatives. http://docs.house.gov/meetings/HM/HM12/20131030/101429/HHRG-113-HM12-Wstate-StempfleyR-20131030.pdf.
Trend Micro & OAS. 2014. “Trend Micro, Organization of American States Survey Reveals Growing Concern of Cyber Threats against Critical Infrastructure | Government Security News.” April 7. http://gsnmagazine.com/article/44336/trend_micro_organization_american_states_survey_re.
The White House. 2013a. “Executive Order 13636-- Improving Critical Infrastructure Cybersecurity.” *The White House*. February 12. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
———. 2013b. “Executive Order 13636 - Improving Critical Infrastructure Cybersecurity.” http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
———. 2013. “Presidential Policy Directive 21-- Critical Infrastructure Security and Resilience.” Accessed October 12. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
UCB. 2005. “UC Berkeley to Lead $19 Million NSF Center on Cybersecurity Research.” April 11. http://www.berkeley.edu/news/media/releases/2005/04/11_trust.shtml.
U.S. Senate PSI. 2012. “Federal Support for and Involvement in State and Local Fusion Centers.” Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs.

http://www.hsgac.senate.gov/download/report_federal-support-for-and-involvement-in-state-and-local-fusions-centers.
WECC. 2012. “September 8, 2011 Southwest Outage Event: Backgrounder.” https://www.wecc.biz/Corporate/FERCOrder_Backgrounder.pdf.