ARTICLE

CYBERSECURITY POLICY FOR THE ELECTRICITY SECTOR: THE FIRST STEP TO PROTECTING OUR CRITICAL INFRASTRUCTURE FROM CYBER THREATS

ZHEN ZHANG[*]

"We can only see a short distance ahead, but we can see plenty there that needs to be done."[1]

Alan Turing

ABSTRACT

Electricity forever changed the dark nights. Without the human ingenuity that harnessed energy in the form of electricity, our world would be very different. Computers and information technology would have never become part of our social fabric. Today, no country is more reliant on information technology and electricity than the United States. Due to these inter-dependencies, cybersecurity threats can compromise the critical infrastructure foundation of the United States. In light of this, the electricity sector is among the only critical infrastructure sectors with mandatory cybersecurity standards. This Article focuses on cybersecurity in the context of the electricity sector, despite that many of the same challenges exist in other industries as well. Due to the novel aspects of cyber threats, this Article sets the stage by detailing specific characteristics such as the problems of prediction and identification. Cybersecurity has many governance challenges as well. Unclear assignment of responsibility, protecting civil liberties, responses that escalate the situation, and poor access to information on cyber events are all contributing factors. In response to these challenges, this Article proposes five components to a comprehensive cybersecurity policy: (1) recognition of responsibility by the government and the industry; (2) information sharing of cyber threats and vulnerabilities; (3) procurement rules for vendors; (4) federal agency emergency powers; and (5) international cooperation. According to the five components, this Article examines the existing mandatory reliability standards

[*] Zhen Zhang is an attorney specializing in energy and environmental law. She is a policy analyst at the California Public Utilities Commission. Prior to working in California, she was a visiting attorney at Natural Resources Defense Council, Beijing, and a Global Energy Fellow at the Institute for Energy and Environment at Vermont Law School. Zhen also practiced environmental law in Maryland and in Washington, D.C. Zhen received a B.S. in environmental policy at the University of Michigan, a J.D. at the University of Maryland, and an LL.M. in environmental law at Vermont Law School. The content of this Article and the opinions expressed within are hers alone and in no way reflects those of her employer.

[1] Alan M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433, 460 (1950).

created by the North American Electric Reliability Corporation ("NERC") and the proposed cybersecurity laws for the electric grid. Unsurprisingly, neither the existing mandatory cybersecurity standards, nor the proposed laws, create a comprehensive policy. This Article concludes that new regulations and laws should address the shifting leadership roles of the private industry and government, which depend on the timing of the threat and the particular situation. Additionally, changes in both regulations and laws are necessary to create a national-level data aggregator, analysis, and notification center for the electricity sector. Regulatory and legal changes are not necessary for procurement rules because it can be a voluntary program. If procurement rules are mandatory, then NERC standards can be revised to create baseline vendor requirements. Laws are better suited for declaring federal emergency powers and international cooperation. Because the current regulations and laws have not kept up with information technology advancements and cybersecurity, the policy proposed in this Article will bring the United States closer to addressing the unique challenges of cyber threats and protecting our critical infrastructure.

I. INTRODUCTION

The electric grid is crucial to our society and is increasingly dependent on information technology and network systems.[2] Thus, a strong and reliable grid requires strong cybersecurity. The electricity sector is appropriate for cybersecurity analysis because it is among the only critical infrastructure sectors with mandatory cybersecurity standards.[3] These are mandatory reliability standards by NERC, which is the standard setting, auditing, and enforcement entity for the bulk power system, supervised by the Federal Electric Regulatory Commission ("FERC").[4] Similar to the electricity sector,

[2] U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 35 (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[3] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 08-1075R, INFORMATION TECHNOLOGY: FEDERAL LAWS, REGULATIONS, AND MANDATORY STANDARDS FOR SECURING PRIVATE SECTOR INFORMATION TECHNOLOGY SYSTEMS AND DATA IN CRITICAL INFRASTRUCTURE SECTORS 2 (2008) (Figure 1) (noting that of eighteen critical infrastructure sectors, only the related energy and dams sectors have applicable mandatory standards). *Cf.* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 12-92, CRITICAL INFRASTRUCTURE PROTECTION: CYBERSECURITY GUIDANCE IS AVAILABLE, BUT MORE CAN BE DONE TO PROMOTE ITS USE 24, 35 (2011) (claiming that many critical information sectors have mandatory standards by virtue of their federal regulation, but noting that only the electricity sector, depository institutions sector, and the nuclear sector have standards similar to the mandatory standards applicable to federal agencies). For further discussion, *see infra* Part IV.

[4] 16 U.S.C. § 824 (2006); Order Certifying North American Electric Reliability Corporation as the Electricity Reliability Organization and Ordering Compliance Filing, No. RR06-1-000, 116 FERC ¶ 61,062 (Fed. Energy Regulatory Comm'n July 20, 2006), *available at* http://www.ferc.gov/whats-new/comm-meet/072006/E-5.pdf.

other critical infrastructure sectors continue to adopt information technology tools, such as the Internet, for interconnectivity and efficiency.[5] As such, the issues and recommendations associated with reliability standards and cybersecurity of the electric grid are applicable to critical infrastructure protection in general.

The 2003 blackout that affected much of the East Coast and Canada was the biggest factor in making mandatory the previously voluntary electric reliability standards.[6] However, the cybersecurity standards target daily operations, not high-impact, low-probability events.[7] Thus, the current concern is that the electric grid will not be able to withstand a coordinated attack.[8] Government agencies and legislators are struggling with how to address this problem. A broad comprehensive approach is necessary as electricity and information systems are cross-sector industries.

This Article explains in Part II the unique issues associated with cybersecurity. Some are specific to the electric grid and other issues are generally applicable to cybersecurity for any industry.[9] This Article does not

Standards approved by the NERC Board of Trustees, including the Critical Infrastructure Protection Group for cybersecurity, are posted on the NERC website. *See* N. AM. ELECTRIC RELIABILITY CORP., RELIABILITY STANDARDS FOR THE BULK ELECTRIC SYSTEMS OF NORTH AMERICA (2013), *available at* http://www.nerc.com/docs/standards/rs/Reliability_Standards_Complete_Set.pdf.

[5] *Compare* Pikkarainen et al., *Customer Acceptance of Online Banking: An Extension of Technology Acceptance Model*, 14 INTERNET RES. 224 (2003) (analyzing the shift to online banking in recent years), *with* Robin Sidel, *Banks Make Smartphone Connection*, WALL ST. J., Feb. 11, 2013, http://online.wsj.com/article/SB10001424127887323511804578298192585478794.html (discussing mobile phone banking such as using the cell phone pictures to deposit checks). *See also* OFFICE OF ELEC. TRANSMISSION & DISTRIB. U.S. DEP'T OF ENERGY, "GRID 2030": A NATIONAL VISION FOR ELECTRICITY'S SECOND 100 YEARS 13 (2003) [hereinafter GRID 2030], *available at* http://www.climatevision.gov/sectors/electricpower/pdfs/electric_vision.pdf.

[6] *See* U.S.-CAN. POWER SYSTEM OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA 140 (2004) [hereinafter 2003 BLACKOUT FINAL REPORT], *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf.

[7] N. AM. ELECTRIC RELIABILITY CORP., HIGH-IMPACT, LOW-FREQUENCY EVENT RISK TO THE NORTH AMERICAN BULK POWER SYSTEM 3 (2010) [hereinafter NERC HILF REPORT], *available a*t http://www.nerc.com/files/HILF.pdf (stating that the electric sector has been successful in managing day-to-day reliability); Mark Weatherford, Chief Sec. Officer, N. Am. Electric Reliability Corp., Presentation at The Energy Bar Association's "How Secure is the Grid?" (Apr. 6, 2011) [hereinafter Weatherford Presentation] (stating that standards are for long-term static situations) (notes on file with author).

[8] N. AM. ELECTRIC RELIABILITY CORP., CRITICAL INFRASTRUCTURE STRATEGIC ROADMAP 5 (2010) [hereinafter CRITICAL INFRASTRUCTURE ROADMAP], *available at* http://www.nerc.com/docs/escc/ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf.

[9] *See infra* Part II.

cover the unlimited range of cybersecurity challenges, but it highlights relevant examples to provide context for the five necessary components of a successful cybersecurity policy. Part III describes in detail these five components: (1) recognition of responsibility; (2) information sharing; (3) procurement rules; (4) emergency powers; and (5) international cooperation.[10] Following the description of the five components, Part IV examines NERC's cybersecurity standards, and how these standards fail to support all five policy components.[11] Part V describes three proposed laws that remedied some, but not all, of the deficiencies.[12] In Part VI, the Article concludes with a summary of the five components and how some components require both regulatory and legal changes, while other components only need one or the other.[13]

This Article suggests improvements for the current regulatory and legal framework to help industry and policy makers set clear objectives for protecting the United States' critical infrastructure. It does not diminish the fact that NERC's standards, as one of only a few federally mandated cybersecurity standards for a critical infrastructure sector, are part of a solid first step. Indeed, given the increasing importance of critical infrastructure protection, the cybersecurity standards could have cross-sector application, such as within the manufacturing industry and the information technology industry.[14]

II. BACKGROUND

If the critical infrastructure sectors are not protected from harm and damage, then the "national economic security, and national public health or safety" can topple like a row of dominos or collapse all together.[15] In 1998, President Bill Clinton identified electric power as one of the critical infrastructure sectors.[16]

---

[10] *See infra* Part III.

[11] *See infra* Part IV.

[12] *See infra* Part V.

[13] *See infra* Part VI.

[14] Zhen Zhang, *NERC's Cybersecurity Standards: Fulfilling Its Reliability Day Job and Moonlighting as a Cybersecurity Model*, 13 ENVTL. PRAC. 250, 257–61 (2011).

[15] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 § 1016, 42 U.S.C. § 5195c (2006).

[16] Presidential Decision Directive 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The most recent Presidential Policy Directive 21 listed sixteen critical infrastructure sectors: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waster, transportation systems, and water and wastewater systems. Presidential Policy Directive 21 (Feb. 12,

Without electricity, other critical infrastructure sectors such as banking and finance, emergency services, and government facilities would be incapacitated.[17] Financial markets would close and military operations would be delayed.[18] These cross sector dependencies show that preserving the electric supply is a basic requirement of our daily life activities, social stability, and national security.[19]

A. Reliability Versus Security

Reliability and security are two distinct concepts even though the terms are often used interchangeably. The electric industry needs to recognize the differences and plan accordingly in order to formulate appropriate protections. Reliability means consistent operation in the face of disturbances and ensuring an adequate flow of power to consumers.[20] The main goal of reliability is keeping the lights on by preventing events that cause outages. It could involve activities such as balancing load or reactive power.[21]

On the other hand, security does not necessarily affect operations immediately. Security means preventing unintentional distribution of information about the control system.[22] For instance, while protecting an employee's personal information seems to have little immediate operational effect, disclosures may weaken overall system integrity.[23] Security is different from reliability in that it provides increased protection for the control systems

2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[17] NAT'L INFRASTRUCTURE ADVISORY COUNCIL, PRIORITIZING CYBER VULNERABILITIES 8 (2004) [hereinafter PRIORITIZING CYBER VULNERABILITIES], *available at* http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf; Mark Weatherford, *Securing the North American Electric Grid*, GOV'T TECH. (Jan. 4, 2011), http://www.govtech.com/technology/Securing-the-North-American-Electric-Grid.html.

[18] *Securing the Modern Electric Grid from Physical and Cyber Attacks: Hearing on H.R. 2195 Before the Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology of the H. Comm. on Homeland Sec.*, 111th Cong. 10, 11 (2009) [hereinafter *Hearing on H.R. 2195*] (statement of William R. Graham, Chairman, Comm'n to Assess the Threat to the United States from Electromagnetic Pulse).

[19] *Id.*; PRIORITIZING CYBER VULNERABILITIES, *supra* note 17, at 8 (2004) (finding that all critical infrastructure sectors depend on information technology and network systems).

[20] 2003 BLACKOUT FINAL REPORT, *supra* note 6, at 1; 16 U.S.C. § 824o (2006).

[21] Jack Danahy & Andy Bochman, *Attention Congress: A Grid Needs a New Virtue*, SMARTGRIDNEWS.COM (Apr. 6, 2010), http://www.smartgridnews.com/artman/publish/Technologies_Security/Attention-Congress-A-New-Grid-Needs-a-New-Virtue-2111.html.

[22] IDAHO NAT'L ENG'G AND ENV'L LAB., U.S DEP'T OF HOMELAND SEC., A COMPARISON OF ELECTRICAL SECTOR CYBER SECURITY STANDARDS AND GUIDELINES 1 (2004).

[23] *Id.*

responsible for sending directions to grid components.[24] In addition, security means ensuring that not only are assets always available, but also that the assets are protected from misuse.[25]

Security encompasses both cybersecurity and physical security.[26] Physical security can be as broad as installing fences around substations or hiring private patrol teams. This Article focuses on cybersecurity, any discussion of physical security involves physically securing the cyber assets, as required by NERC standards.[27]

B. Cybersecurity of the Electric Grid

The NERC cybersecurity standards, adopted in 2003, became mandatory in 2008.[28] Electric infrastructure was one of the last sectors to become electronically automated despite maintenance and updates on its poles and wires over the years.[29] It is still in the midst of changing from a mechanical system to an automated system.[30] The electric grid is more dependent on information technology as companies incorporate digital and information technology networks to increase communication for automated functions.[31] Increased communication is necessary as the electric grid accommodates

---

[24] *Id.*

[25] *Hearing on H.R. 2195*, *supra* note 18, at 25 (statement of Michael J. Assante, Chief Security Officer, North American Electric Reliability Corporation).

[26] *Id.* at 2 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.).

[27] Mandatory Reliability Standards for Critical Infrastructure Protection, 72 Fed. Reg. 16,461 (Mar. 16, 2007) (to be codified at 18 C.F.R. pt. 40); Mandatory Reliability Standards for Critical infrastructure Protection, No. RM06-22-000, 122 FERC ¶ 61,040 (Fed. Energy Regulatory Comm'n Jan. 18, 2008) *available at* http://www.ferc.gov/whats-new/comm-meet/2008/011708/e-2.pdf; *see also* N. AM. ELECTRIC RELIABILITY CORP., GUIDANCE FOR ENFORCEMENT OF CIP STANDARDS 1 (2008), *available at* http://www.nerc.com/files/Guidance_on_CIP_Standards.pdf.

[28] FED. ENERGY REGULATORY COMM'N, FERC USE OF THE GRID RELIABILITY APPROPRIATION FOR FISCAL YEAR 2004 14 (2004) [hereinafter FERC APPROPRIATION 2004], *available at* http://www.ferc.gov/industries/electric/indus-act/reliability/reliability-rpt-fnl.pdf; Mandatory Reliability Standards for Critical Infrastructure Protection, 72 Fed. Reg. 16,461.

[29] Dan Ton, Program Manager, Smart Grid Research & Dev., Presentation at UCLA HSSEAS Smart Grid Seminar Series (Nov. 19, 2009) (presentation slides available at http://www.ita.ucla.edu/news/presentations/Ton-UCLA1119-rv.pdf) (stating that one of the functions of the smart grid is to replace previously manual functions with digital tools).

[30] GRID 2030, *supra* note 5, at 13–14.

[31] *Hearing on H.R. 2195*, *supra* note 18, at 12 (statement by Mark Fabro, President and Chief Security Scientist, Lofty Perch) (stating that the electric grid will continue to converge with Internet based systems as it matures, and it will inherit similar vulnerabilities).

renewable power sources and enables new technology like smart meters and plug-in hybrid electric vehicles.[32] Much of the technology uses the Internet or intranets that can be accessed from the Internet.[33]

These new connections to the Internet transfer many of the problems that affect personal computers to grid operation programs.[34] Without cybersecurity, the loss of the electric grid can be catastrophic.[35] Security protection measures must mitigate the effects of intentional or unintentional cyber events. The key questions that must be answered are: what protections should be in place and what are the appropriate responses?[36]

There is a general impression that the electric grid is not secure against cyber attacks and catastrophic events.[37] The private sector is responsible for maintaining a continuous flow of electricity and they must comply with NERC standards.[38] The House Committee on Homeland Security reviewed NERC standards, concerns, and issues for proposed bills to improve grid security. It concluded that the private electric industry has not secured the grid.[39] In fact, the House Committee found that the industry is avoiding compliance with the mandatory standards.[40] Interestingly, the energy industry executives see their industry as the most prepared against cyber attacks in a survey of over 1,580 companies worldwide.[41]

---

[32] GRID 2030, *supra* note 5, at 17–21.

[33] *See Hearing on H.R. 2195*, *supra* note 18, at 12 (statement by Mark Fabro, President and Chief Security Scientist, Lofty Perch) (stating that the electric grid will continue to converge with Internet based systems as it matures, and it will inherit similar vulnerabilities).

[34] Weatherford, *supra* note 17.

[35] *Hearing on H.R. 2195*, *supra* note 18, at 2 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.).

[36] *Id*. at 3.

[37] *Id*.; Jeanne Meserve, *'Smart Grid' may be Vulnerable to Hackers*, CNN.COM (Mar. 21, 2009, 12:44 AM), http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/.

[38] *Hearing on H.R. 2195*, *supra* note 18, at 3 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.); 16 U.S.C. § 824o (2006).

[39] *Hearing on H.R. 2195*, *supra* note 18, at 3–4 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.); Letter by Michael Assante, Vice President and Chief Security Officer of N. Am. Electric Reliability Corp., to Industry Stakeholders (Apr. 7, 2009), *available at* http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

[40] *Hearing on H.R. 2195*, *supra* note 18, at 3–4 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.).

[41] SYMANTEC, SYMANTEC 2010 CRITICAL INFRASTRUCTURE PROTECTION STUDY: GLOBAL RESULTS (2010), *available at* http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf; *Hearing on H.R. 2195*, *supra* note 18, at 33

The current urgency to pass a law dealing with cybersecurity protection of the electric grid is based on the anticipation of a large-scale organized cyber attack.[42] When creating a response plan however, one must examine the protections already in place.[43] The grid needs comprehensive protections from the continuum of cyber events, which range from every day threats to cyberwarfare.[44] Before discussing what should be part of a comprehensive cybersecurity policy for the electric grid, this Article looks at cyber threats and the unique challenges of cyber vulnerabilities.

C. Cyber Threats to the Electric Grid are Real

There are many definitions of cyber threats, and this Article takes an expansive view. Cyber threats can be unintentional, such as operating system errors or employee mistakes. They can also be the product of intentional actions by persons who try to access and control a communication system, such as computers, networks, and industrial control systems for destructive purposes.[45] Cyber threats can damage technology, hardware, software, and protocols that make up the essential core control systems of the electric grid. More connectivity between the different grid components means that the threats may result in compound effects on the entire system, which then can cause regional cascading failures lasting for days.[46] Ironically, twenty years ago computer scientists worked hard to establish connectivity between computers, but in the late 1990s the challenge was to separate network

(statement by Mr. Steven T. Naumann, Vice President, Wholesale Mkts, Exelon Corp., Representing Edison Electric Inst. and Electric Power Supply Ass'n) (The North American grid is well protected against known cyber threats); *cf. Communications Industry Sees Itself as Less Prepared for Cyber Attacks*, INFOSECURITY.COM (Oct. 7, 2010), http://www.infosecurity-us.com/view/13071/communications-industry-sees-itself-as-less-prepared-for-cyber-attacks/.

[42] *Hearing on H.R. 2195*, *supra* note 18, at 2–3 (statement by Rep. Yvette D. Clarke, Chairwoman of the Subcomm. on Emerging Threats, Cybersecurity, and Sci. and Tech.).

[43] *Id.*

[44] NAT'L SEC. TELECOMM. ADVISORY COMM., INFO. ASSURANCE TASK FORCE, ELECTRIC POWER RISK ASSESSMENT (1997), *available at* http://www.solarstorms.org/ElectricAssessment.html.

[45] CRITICAL INFRASTRUCTURE ROADMAP, *supra* note 8, at 3; EDWARD G. AMOROSO, CYBER ATTACKS: PROTECTING NATIONAL INFRASTRUCTURE 132–33 (2010) (stating that regardless of security measures, humans are a critical link in the security chain); RICHARD A. CLARK & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 1–16 (2010); U.S. Dep't of Homeland Sec., *Cyber Threat Source Description*, ICS-CERT, http://www.us-cert.gov/control_systems/csthreats.html (last visited Feb. 18, 2013) (focusing on threats from governments, terrorists, spies, and hackers).

[46] *Hearing on H.R. 2195*, *supra* note 18, at 13 (statement of Mark Fabro, President and Chief Sec. Scientist, Lofty Perch).

connectivity for security purposes.[47] Open source information increased the risk of electronic attacks and the impact of hackers.[48] After identifying the problem almost twenty years ago, there is greater recognition of the danger of cyber threats today.[49] The struggle to find solutions continues.[50]

D. SCADA—Critical Infrastructure Control Systems

Companies operating critical infrastructures use Supervisory Control and Data Acquisition ("SCADA") systems to send and receive signals from different devices at different locations.[51] SCADA systems send signals to devices via the network or a radio signal. Electric companies use SCADA systems for everything from generators to substations.[52] Security is a problem because many of these devices are connected to a wireless network or to the Internet.[53] Even if the devices only connect to an intranet, the intranet could connect to the public Internet.[54] The public Internet connection can be used by a hacker to control electric grid devices via the SCADA systems.[55] So far, there have been no publicly available examples of a hacker taking over portions of the electric grid.[56] Regardless, there have been some events that show that the electric industry must be ready to protect the electric grid and the

[47] AMOROSO, *supra* note 45, at 53.

[48] NAT'L SEC. TELECOMM. ADVISORY COMM., *supra* note 44.

[49] Bruce Schneier, *Cyberwar Treaties*, SCHNEIER ON SECURITY (June 14, 2012), http://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html (stating that cyber threats could be cyberwar activities when considering the cumulative impacts).

[50] SYMANTEC, *supra* note 41, at 5 (finding that the private sector recognizes cyber attacks as a serious problem); SYMANTEC, SYMANTEC 2011 CRITICAL INFRASTRUCTURE PROTECTION SURVEY: GLOBAL FINDINGS (2011), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/symc_critical_infrastructure_protection_survey_2011.pdf (finding that organizations feel less prepared in general).

[51] *NERC Issues AURORA Vulnerability Guidelines*, POWERMAG.COM (Oct. 20, 2010), http://www.powermag.com/POWERnews/3106.html.

[52] CLARK & KNAKE, *supra* note 45, at 98–99.

[53] FERC APPROPRIATION 2004, *supra* 28, at 14.

[54] NATIONAL SCADA TEST BED, U.S. DEP'T OF ENERGY, STUDY OF SECURITY ATTRIBUTES OF SMART GRID SYSTEMS—CURRENT CYBER SECURITY ISSUES 12 (April 2009), *available at* http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf (stating that attackers can use wireless networks that support smart meters and sensors to communicate to network devices and directly compromising control systems).

[55] *Id.*; CLARK & KNAKE, *supra* note 45, at 98–99 (noting approximately six SCADA software programs are available commercially).

[56] SANS INST. INFOSEC READING ROOM, CAN HACKERS TURN YOUR LIGHTS OFF? 2 (2001), *available at* http://www.sans.org/reading_room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack_606.

flow of electricity.

For example, operators reported a software glitch in SCADA systems immediately before the cascading effects of the 2003 United States/Canada blackout.[57] Around the same time, a malware virus named the Blaster worm infected SCADA systems to slow down controls.[58] If the software glitch reported in the 2003 blackout was the Blaster worm, and if the control system operators were aware of the dangers the worm posed and knew that it was necessary to strengthen the system against it, then such knowledge and the appropriate actions could have alleviated the severity and extent of the 2003 blackout. In 2004, there were at least forty-eight new software vulnerabilities per week around the world.[59] In 2010, another malware, the Stuxnet worm, targeted SCADA systems specifically.[60] By 2011, there were 403 million unique variants of malware, a forty-one percent increase from the 2010 level.[61] Beyond SCADA systems, cyber vulnerabilities exist across the power delivery system. Eighty-five percent of the electric grid system relays are digital.[62]

Cyber threats also include computer code left behind by hackers, which someone might activate later to disrupt operations or export proprietary information. In 2009, Chinese hackers allegedly penetrated the U.S. electric grid, leaving behind code that if activated could control the grid.[63] In fact,

---

[57] Bruce Schneier, *Internet Worms and Critical Infrastructure*, CNETNEWS.COM (Dec. 9, 2003, 12:00 PM), http://news.cnet.com/2010-1001-5117862.html [hereinafter Schneier I] (noting the glitch related to the "alarm and logging software"); Bruce Schneier, *Blaster and the Great Blackout*, SALON.COM (Dec. 16, 2003, 3:30 PM), http://www.salon.com/2003/12/16/blaster_security/ [hereinafter Schneier II] (stating that it is reasonable to suspect that the MSBlast worm, which caused many computers to crash when it appeared a few days before the 2003 blackout, to be a contributing factor to a computer alarm function failure and backup failure at FirstEnergy).

[58] CLARK & KNAKE, *supra* note 45, at 99.

[59] SYMANTEC, SYMANTEC INTERNET SECURITY THREAT REPORT 2, 4, 24 (Dean Turner & Stephen Entwisle eds., 6th vol. 2004), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_vi.pdf.

[60] Gregg Keizer, *Is Stuxnet the "Best" Malware Ever?*, COMPUTERWORLD.COM (Sep. 16, 2010, 6:47 AM), http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.

[61] SYMANTEC, INTERNET SECURITY THREAT REPORT (Paul Wood ed., 17th vol. 2012), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

[62] NERC HILF REPORT, *supra* note 7, at 31.

[63] CLARK & KNAKE, *supra* note 45, at 59; Siobhan Gorman, *Electric in US Penetrated by Spies*, WALL ST. J., Apr. 8, 2009, http://online.wsj.com/article/SB123914805204099085.html. 'Trap doors' are lines of code that allow unauthorized access without alarming the owner. CLARK & KNAKE, *supra* note 45, at 91. Logic bombs are software applications that in their most basic form are erasers that erase all software on a

during audits, U.S. cybersecurity auditing firms successfully hacked into U.S. grid control systems from the Internet.[64] Another well-known example is the Aurora experiment at the Idaho National Laboratory. There, computer commands were used to instruct a generator to malfunction.[65] Furthermore, hackers can leave behind espionage programs that they control remotely, recording conversations, exporting images, and copying documents.[66] Oil companies, defense companies like Northrop Grumman, and Google have all reported loss of proprietary data.[67] Although one cannot say for sure how the information ended up in a foreign server, espionage programs could have played a role.

E. Challenges of Cybersecurity

Cybersecurity protects computer or network systems and improve their ability to respond to employee errors and contingencies from unknown or hostile sources that cause information leaks and/or corrupt data.[68] Cybersecurity protects a system from becoming unavailable, unusable, and being manipulated by a third party. Cybersecurity has both technical and governance challenges. The complexity of the electric grid and the wide variety of components give rise to purely technical challenges. Cyber events are difficult to predict, plan for, and identify in such a complex environment, especially if the events do not disrupt operations. The source is also difficult to discover. Governance challenges are many, due to the lack of direction, leadership, or vision. Specifically, an unclear assignment of responsibility, the need to protect civil liberties, the escalation problem, and the lack of information all complicate the task of governance. Below, subpart 1 examines the technical challenges, and subpart 2 examines the governance challenges.

---

computer, leaving the computer useless. Logic bombs can order hardware to do something that damages itself, such as producing a surge that fries circuits in transformers, then it erases everything, including itself. *Id*. at 92.

[64] CLARK & KNAKE, *supra* note 45, at 167–68.

[65] *Id*. at 100; COMMITTEE ON OFFENSIVE INFORMATION WARFARE, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 113 (Willa A. Owens et al. eds., The National Academies Press 2009); *NERC Issues AURORA Vulnerability Guidelines*, *supra* note 51.

[66] CLARK & KNAKE, *supra* note 45, at 59.

[67] *Id*. at 60 (noting that Google found on a server in Taiwan with copies of proprietary information from Adobe, Dow Chemicals and Northrop Grumman). Russia allegedly stole technology for automated pump and valve controls to manages oil and gas pipelines. *Id*. at 93.

[68] Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 172–73 (2008); COMMITTEE ON OFFENSIVE INFORMATION WARFARE, *supra* note 65, at 9.

1. Technical Challenges

Electric grid asset owners and operators use diverse technologies, protocols, operating systems, and communication procedures to support the reliability and operation of their specific functions.[69] Coordination is essential to regional and national grid stability. In addition, legacy systems must be taken into consideration when implementing cybersecurity programs, as the old systems may not produce usable data for the new programs. Control systems complicate matters because they must always be available, which may preclude certain countermeasures.[70] In addition, cybersecurity events are difficult to predict and plan for. Similarly, the attribution problem is another unsolved technical challenge. As discussed in Part III, below, procurement rules can address these technical issues.[71]

i. Prediction and Planning Difficulties

Cyber events are difficult to predict, plan for, and identify.[72] Prediction requires prior or current knowledge indicating the likelihood of future events, but information on threats often becomes available only minutes before a threat emerges.[73] Computer vulnerabilities are often made public based on the presumption that vulnerabilities can be addressed and repaired more quickly by the information technology community at large. The reality is, however, that in many cases potential solutions are accompanied by new challenges. Within minutes of the threat announcement, hackers often release destructive code.[74] Accordingly, the electric industry must respond to new threats immediately. Response decisions, including remediation measures such as isolating the compromised system and switching to a backup, must be made on the spot.

Espionage activities are less obvious than cyber events that directly affect operations. These activities are difficult to detect not only because hackers are adept at masking their infiltration into the programs and the changes to the programs, but also because companies often do not know what they are looking for. Remotely controlled programs could have been copying and

[69] *Hearing on H.R. 2195*, *supra* note 18, at 29.

[70] *Id*. at 16.

[71] Weatherford Presentation, *supra* note 7.

[72] Schneier I, *supra* note 57 (stating that it is possible that the computer worms that infected Microsoft operating systems contributed to the 2003 blackout, "[a]s networked computers infiltrate more and more of our critical infrastructure, that infrastructure is vulnerable not only to attacks but also sloppy software and sloppy operations"); Schneier II, *supra* note 57 (stating that accidental failures of support systems, such as alarms and remote controls, are more likely than directed cyber attacks).

[73] PRIORITIZING CYBER VULNERABILITIES, *supra* note 17, at 4.

[74] *Id*.

exporting information without discovery for days, months, or even years.[75] Preventing the loss of proprietary and operations information to parties with malicious intent must be part of the long-term security plan of any system.

ii. The Attribution Problem

A wide variety of actors can generate cyber events. They could be the result of careless employees, vendors, or thrill seeking individuals.[76] Perhaps the most serious events are coordinated activities targeted at disabling the electric grid by terrorist sympathizers, terrorists, and nation-states.[77] There are no geographic borders in cyber space.[78] Perpetrators can create and insert their programs from anywhere, remotely activating programs installed months ago.[79] Even with today's diagnostic tools, attackers can hide their location making it difficult to identify the source of the incident.[80]

Cyber threats are unpredictable and volatile. The electric industry cannot manage on its own the difficulty with identifying the source of the threat. As such, government has an important role, which includes providing guidance so that the industry does not take actions contrary to national interests. For instance, it may be important to tailor the response depending on whether the attack came from a nation-state or a terrorist group. The government can assist private industry by directing their response activities pursuant to the government's emergency powers or creating international legal assistance treaties to extradite a perpetrator. Part III, below, expands upon these ideas.

2. Governance Challenges

Due to the wide range of cyber events, the division of responsibility remains murky between the private electric industry and government. Researchers and

[75] CLARK & KNAKE, *supra* note 45, at 59 (discussing the discovery of a highly sophisticated computer program, dubbed GhostNet by Canadian researchers, that remotely took control of an estimated 1,300 computers at several countries' embassies in 2009).

[76] *See* INST. FOR SEC. TECH. STUDIES AT DARTMOUTH COLL., CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS 12 (2001), *available at* http://www.ists.dartmouth.edu/docs/cyber_a1.pdf.

[77] *See id*.

[78] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

[79] *Hearing on H.R. 2195*, *supra* note 18, at 22, 63–64.

[80] COMPUTER SCI. & TELECOMMS. BD., NAT'L ACAD. OF SCIS., CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 4 n.9 (2002), *available at* http://books.nap.edu/html/cybersecurity/ (stating that tracing attacks is difficult because serious attackers are "likely to launder their connections to the target. . . . [A]n attacker will compromise some intermediate targets whose vulnerabilities are easy to find and exploit, and use them to launch more serious attacks on the ultimate intended target").

electric grid operators should be aware of the impact on civil liberties when gathering and aggregating information about cyber events. Escalation risks exist when a response has more severe impacts than the original cyber event. Governance challenges indicate that current law has not caught up with the unique and evolving characteristics of cybersecurity.

i. Unclear Assignment of Responsibility

There is a spectrum of cyber events, ranging from employee mistakes, non-directed viruses, to misinformed control centers, to the worst: "highly-coordinated, well-planned, attacks against multiple assets designed to disable the system."[81] The highly-coordinated attack may be on multiple critical infrastructure sectors simultaneously, the electric grid being only one of the sectors affected. Many regard the highly-coordinated cyber attack as a national security issue, the responsibility of which resides with the federal government.[82]

For the electric sector, mandatory reliability standards require it to manage at least the day-to-day reliability risks.[83] There is no clear legal mandate that the industry has the responsibility of preventing and responding to cyber attacks, but there is industry awareness and acceptance that the industry's security measures are the first line of defense.[84] At least for the larger entities, it appears that the electric sector has voluntarily acknowledged its responsibilities for pre-event mitigation measures that protect the grid from a wide range of cyber events.[85] The confusion increases in the period following the cybersecurity event. Many factors, such as identifying a specific event, categorizing the event in a legal sense to determine jurisdiction, the impact of the event, information regarding the source, all affect whether federal agencies will be involved.[86] It is in the post-event period that both the government and

[81] NERC HILF REPORT, *supra* note 7, at 26; *see also* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 440 (2009); Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 300–01 (2008) (distinguishing between cyber attacks, which include cyber terrorism and cyber warfare, and cyber crimes for financial or personal gain).

[82] Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 218–19 (2009).

[83] NERC HILF REPORT, *supra* note 7, at 3, 9.

[84] W. Michael Susong, Dir., Info. Sec. Intelligence, Pac. Gas & Elec. Co., Presentation at the Critical Infrastructure Symposium (Apr. 30, 2011) [hereinafter Susong Presentation] (presentation slides available at http://www.tisp.org/index.cfm?cdid=12161&pid=12081) (notes on file with author).

[85] *Id*.

[86] *See* Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in*

the industry must have a clear understanding of their individual and combined responsibilities. Part III, below, discusses this issue in detail.

ii. Civil Liberties

If a government entity bears the responsibility to respond to a cybersecurity event, the response must be sensitive to U.S. civil liberties. Defense measures can be passive or active. Passive defense involves activities such as strengthening the system via encryption and firewalls and educating users to behave properly to prevent and minimized impacts or facilitate recovery from a threat.[87] In contrast, active defense would neutralize a perpetrator's ability to attack and create immediate consequences to the attacker, such as sending back destructive viruses.[88] There are publicly available active defense tools today.[89] These tools are dangerous, however, because active defense measures may infringe upon U.S. civil liberties.[90]

In the United States, citizens expect the right to privacy, the right to protection against unreasonable searches, and the right to due process.[91] Passive defenses such as encryption and firewalls do not violate these rights.[92] Alternatively, active defenses may violate a person's civil liberties by entering a person's realm of privacy and private property, gathering information from the person's computer, or destroying equipment.[93] Because the government entity must respond immediately in order to preserve operation of a critical infrastructure asset, it is hard to predict which civil rights might be violated at the moment of decision making.[94]

Even when a private, non-governmental, entity bears responsibility to respond, that entity must be careful to balance its responsibilities to keep the lights on with its risk of liability for the responses. Although an active defense may be considered defense of property or a matter of necessity, an active defense that is overly aggressive may expose an operator to tort and criminal liability. Preparation, prior research, and the creation of protocols would

Cyberspace, 20 HARV. J. L. & TECH. 403, 417 (2007).

[87] Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 21–24 (2009).

[88] *Id*. at 25.

[89] *Id*. at 21–22 (noting under the prevailing interpretation of the law of war, active defenses against cyber attacks are prohibited).

[90] Condron, *supra* note 86, at 416–17 (explaining that parties that take active defenses against U.S. citizens may violate civil liberties).

[91] U.S. CONST. amends. IV, V, XIV.

[92] Condron, *supra* note 86, at 417.

[93] *Id*.

[94] *Id*.

minimize legal liabilities. Some private industry members do not have the resources or expertise to deal with complex issues; therefore, the industry needs guidance and assistance from the government.

iii. The Escalation Problem

If an active defense is used to repel a cyber attack, then the response to a cyber event may unlawfully escalate the situation. For instance, an active preemptive defense may violate U.S. civil liberties by copying material from a private computer.[95] An active defense may also damage property, which can result in a civil lawsuit or criminal charges.[96] Even if the attack originated from outside the United States, U.S. laws may apply if a party in the United States was the perpetrator or the victim.[97]

International law of armed warfare applies if the cyber attack is the most damaging type, meaning that it reaches the severity of traditional armed warfare.[98] The consequences of such an attack can shut down services, damage property, cripple society, and perhaps even cause loss of life.[99] Despite some well-documented cyber attacks as part of military movements, international law of armed warfare for cyber warfare is just developing.[100] Under traditional international law of armed warfare, defensive measures are appropriate in limited circumstances.[101] Similarly, in order for a country to respond to a cyber attack in self-defense, it must show three elements: necessity, proportionality, and immediacy.[102] Necessity requires the responding party to attribute the attack to an actor.[103] As discussed above, identifying the perpetrator is no easy task.[104] If the response occurred before attribution and was disproportionately destructive compared to the original cyber attack, then it could be concluded that the response was unnecessary. As a result, the entity would have launched an illegal cyber attack inadvertently.[105] Sometimes defense measures can result in provocative

[95] *Id*. at 416–18.

[96] *See* Sklerov, *supra* note 87.

[97] Shackelford, *supra* note 82, at 218–19.

[98] *Id*.

[99] *Id*.

[100] *See* CLARK & KNAKE, *supra* note 45, at 1–16; Condron, *supra* note 86, at 413–16.

[101] Condron, *supra* note 86, at 412.

[102] *Id*. at 413.

[103] *Id*. at 413–14.

[104] COMPUTER SCI. & TELECOMMS. BD., NAT'L ACAD. OF SCIS., *supra* note 80, at 4 n.9 (noting that tracing attacks is difficult because serious attackers will hide their connections to the main target by compromising intermediate targets and then use the intermediates to launch serious attacks on the ultimate target).

[105] Condron, *supra* note 86, at 414–15.

activities that increase the likelihood of conflict.[106] Even if there is proportionality and immediacy, the activity cannot be legitimate without necessity.

Both civil liberties laws and international warfare laws raise complex legal questions. Allowing private industry to act without government support in such an environment could damage national security and political relationships. Domestic government guidance via emergency powers is necessary in national security situations and would be a welcomed resource to private industry. On the international front, there are many efforts to develop warfare laws that address the unique aspects of cyber events. Part III, below, discusses how international cooperation can help.

iv. Lack of Information

In defending the grid from threats and creating remedies and situational awareness, we rely heavily on data. Data analysis results in useful information, such as predicting threats and uncovering vulnerabilities.[107] Currently there is a lack of data and a lack of useful information.[108]

Legal and institutional barriers discourage sharing data for research. The Electronic Communications Privacy Act ("ECPA") does not have a research exception to the prohibition against gathering emails, Internet usage histories, and instant messaging.[109] The potential for legal liability also discourages entities from sharing data outside its organizational lines.[110] Consequently, cybersecurity research is conducted within one's organization and these individualized solutions could prevent coordination and inhibit solutions for the electric industry as a whole.[111] Consumer disapproval and negative publicity are concerns as well.[112]

Another barrier is creating information useful to the electric industry from a

[106] CLARK & KNAKE, *supra* note 45, at 155.

[107] AMOROSO, *supra* note 45, at 154–55 (stating that collecting system data, such as audit log information, from multiple sources for cybersecurity is necessary for security analysis, but barriers include cost, legal issues, and discomfort over proprietary or sensitive data).

[108] Burstein, *supra* note 68, at 170–71.

[109] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[110] Burstein, *supra* note 68, at 187; *see also Hearing on H.R. 2195*, *supra* note 18, at 13 (stating that research that "promotes the independent assessment of power system technologies without legal consequences or negative attributions is necessary," and that research must "include information sharing and cyber incident response functions so that we can better prepare for, detect and respond to incidents unique to bulk power system architectures").

[111] Burstein, *supra* note 68, at 171–72.

[112] *Id*. at 197.

countless variety of data. Data in itself is often meaningless. Only after it is analyzed and interpreted can it provide the industry with potential cybersecurity tools. As indicated by the discussion above regarding the diverse nature of the grid, there is no one-size-fits-all virus detection program or mitigation strategy.[113] Nevertheless, a national-level, real-time situational awareness analysis would be very useful to grid operators by giving them the ability to understand the normal business as usual status as compared to the current status.[114] Earlier warnings mean more opportunities to respond before there is damage to assets and operations.[115] Coordination between the government and private industry is necessary to create an accurate and complete view of current cyber risks.[116] So far there is no national-level situational awareness program.[117] Part III, below, discusses the benefits of creating a national-level data compilation, research, analysis, and alert center.

III. THE FIVE COMPONENTS OF A COMPREHENSIVE CYBERSECURITY POLICY

Given the challenges described above, this Article introduces the five components of a successful cybersecurity policy for the electric grid: recognition of responsibility, information sharing, procurement rules, emergency powers, and international cooperation.[118]

A. Recognition of Responsibility

Responsibility for cybersecurity should shift between the government and the private industry depending on timing and the circumstances of the cyber event. Pre-event, before any cybersecurity threat has occurred, the private industry is clearly the responsible party for implementing the protective measures. During the post-event period, responsibility should initially be a combination of private industry with government guidance, and then increase the government's role as needed. Ideally, one federal governmental entity would be responsible for cybersecurity and be clearly identified to, and

---

[113] *Hearing on H.R. 2195*, *supra* note 18, at 16.

[114] AMOROSO, *supra* note 45, at 182–83, 190–91.

[115] *Id*. at 190–91.

[116] *Id*. at 192.

[117] *Id*.

[118] *See* WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009) [hereinafter WHITE HOUSE CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. The Review discusses all five components in the larger context of cybersecurity for national defense and all critical industries. The general ideas of the five components appear to inform the Review's recommended near-term actions.

accepted by, the electric industry.[119] For example, the U.S. Securities and Exchange Commission oversees all participants of the U.S. security markets in order to "protect investors . . . and facilitate capital formation."[120] Similarly, the Federal Communication Commission is the main organization responsible for creating and implementing policies for private communication companies in the United States and between the United States and other countries.[121]

In the pre-event period, it is important for the industry to recognize that it must look at the bigger picture and engage in an inclusive assessment.[122] While the mandatory NERC reliability standards only create a baseline more suited to daily operations,[123] there is room for the electric industry to perform at least a comprehensive evaluation. A more comprehensive evaluation does not mean spending more money. Assessing security measures in the context of the industry as a whole prevents the private industry from implementing measures that push threats away from individual entities, potentially damaging system security overall.[124] Security measures should be selected based on their ability to support industry wide security. In addition, because industry-implemented cybersecurity measures are the first line of defense against cyber warfare, it should consider the defensive measures' effectiveness in the worst case scenario. Although large utilities and NERC recognize their responsibility to prepare for the worst case scenario, it is unclear if the electricity industry as a whole has acknowledged this responsibility.[125] If all members of the industry make an inclusive assessment and accept responsibility for taking reasonable measures to prepare for the worst-case scenario, then the entire industry will be strengthened.

Responsibility during the post-event period is less clear than during the pre-event period. For the purpose of this Article, the post-event period encompasses the period of time beginning after identification of the event, including when response measures are formulated, and ending when the asset owner mitigates the vulnerabilities susceptible to the threat. Unfortunately, not all cyber threats can be identified immediately if they do not affect

---

[119] *Id*. at iii, 7–11.

[120] Securities Exchange Act of 1934, 15 U.S.C. § 78a–78pp (2006).

[121] Communications Act of 1934, 47 U.S.C. § 151–621 (2006) (creating the Federal Communication Commission ("FCC") and giving the FCC broad authority to regulate).

[122] Annabelle Lee, Technical Exec. for Cyber Sec., Electric Power Research Institute, Presentation at The Energy Bar Association's "How Secure is the Grid?" (Apr. 6, 2011) [hereinafter Lee Presentation].

[123] Weatherford Presentation, *supra* note 7.

[124] Burstein, *supra* note 68, at 171.

[125] NERC HILF REPORT, *supra* note 7, at 8; Susong Presentation, *supra* note 84 (stating that private industry is the first line of defense and PG&E security measures considers a wide range of cyber attacks and terrorist activities).

operations.[126] If the threat does not trigger an immediate response, determining the proper apportionment of responsibility between the private industry and the government is difficult. During the entire post-event period, the industry must have a clear idea of which federal agency is the lead for cybersecurity overall so that the industry can go to that entity immediately for assistance.[127] While FERC is known for its electricity sector expertise, it is not the cybersecurity lead for all critical infrastructure sectors in the United States. Coordinating the operation of infrastructure in the United States as a whole, of which the electricity grid is a part, is important for the country's general state of preparedness. The agency or authority that ultimately holds the emergency power should be supported by flexible regulations to help it determine when and how to exercise its power. This is true for the critical electricity infrastructure in particular, but also for the critical U.S. infrastructure sectors in general. The industry must be prepared for government directives and have the capacity to follow orders.

As the idea that the electric industry is responsible becomes more widely accepted by those in the industry, and as the industry begins to take reasonable steps to prepare for the worst-case scenario, the government should create procedures that make asking for and receiving assistance as easy as possible. Given the industry's importance to the nation, the federal government needs to establish a federal cybersecurity authority. The authority will provide the electric industry with government-guided responses when necessary. The private industry and the government could have shifting leadership roles in the pre-attack or post-attack periods. As long as the roles are understood and accepted by both parties, the shifting roles can be effective.

B. Information Sharing

The electricity industry needs a federally funded information sharing and analysis center to aggregate data and provide the industry with national-level, real-time situational awareness. This will help the industry understand the difference between the business-as-usual and the grid's current state.[128] In the same way energy and power information about the distribution lines are shared with the transmission lines operators in order to balance the generation and load of the electric grid, the status of compromised information technology systems should be shared with a national analysis center/depository as soon as possible.

The center would aggregate data on a consistent and guaranteed basis from

---

[126] *See supra* Part II.

[127] CLARK & KNAKE, *supra* note 45, at 131.

[128] *See* AMOROSO, *supra* note 45, at 145, 176, 183, 190–92.

government and non-government entities.[129] Data from general Internet usage should be made available for research as well, which means current privacy laws, such as the ECPA, must be amended to include research exceptions.[130] The data should be consistent and guaranteed, because if the data is only provided on a best-efforts basis, or sporadically, then researchers may miss patterns and activity profiles.[131] The contributing entities could include research institutions, industry, and government agencies.[132] The Electric Sector-Information Sharing Analysis Center ("ES-ISAC"), which gathers industry information, and the United States Computer Emergency Readiness Team ("US-CERT"), which compiles government information, could participate.[133] Classified and unclassified data together create a comprehensive data set when either data group alone would present an incomplete picture. The center would establish procedures appropriate for classified materials and would serve as a facility for exchanging confidential information.[134] This would address the complaint that more industry members should have security clearance and the fact that some companies lack the protocols or the facilities to receive confidential information even if their employees have security clearance. The center would have expert data interpreters and staff to accept and record security reports.[135] The systems operators can use the information generated by the center to implement pre-

[129] There are information sharing programs, but they are voluntary and the data is not guaranteed or consistent. DHS created the Protected Critical Infrastructure Information ("PCII") program pursuant to the Critical Infrastructure Information Act of 2002. *Protected Critical Infrastructure Information Program*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/editorial_0404.shtm (last visited May 3, 2011). The PCII program allows the private sector to submit confidential information regarding the nation's critical infrastructure to DHS. *Id*. The information itself will be protected from public disclosure and work on the information will be subject to confidentiality and proprietary agreements. *Id*. This is not electricity sector specific. *Id*.

[130] *See generally* Burstein, *supra* note 68.

[131] *Id*. at 176. AMOROSO, *supra* note 45, at 176–77.

[132] *See* AMOROSO, *supra* note 45, at 170. Critics believe there is too much emphasis on information sharing because the presumption that the government or industry can prevent cyber attacks or reduce vulnerabilities is unsupported by industry experience. *See id*. at 134, 135. Similarly, government cyber attack assistance is rare. *See id*.

[133] *Hearing on H.R. 2195*, *supra* note 18, at 30. NERC managed ES-ISAC is immature and still under development. Private industry generally goes to the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") and US-CERT, but these entities cover all control systems for industry. These systems are not electricity sector specific. Interview with Mark Weatherford, Chief Sec. Officer, N. Am. Electric Reliability Corp., in Washington, D.C. (Apr. 11, 2011) [hereinafter Weatherford Interview].

[134] *See* AMOROSO, *supra* note 45, at 154–56.

[135] *Id*. at 190–91.

event protective measures and post-event mitigating measures. [136]

Information sharing does not mean that the mitigating measures used by the government will work for private companies, or vice versa.[137] No one solution can work for the entire industry, nor will one solution protect the grid from all threats.[138] Although finding solutions and sharing best practices are important, the more accessible value of information sharing is improving situational awareness.[139] Depending on national security reasons and industry needs, the center could establish two categories: classified and unclassified situational awareness.[140] Information sharing increases the likelihood of having pre-attack responses as preventative tools to stop problems before they have more serious unanticipated impacts.[141]

C. Procurement Rules

Mandatory or non-mandatory procurement rules would encourage cybersecurity to be built into the system. Vendors already use procurement guidelines as a source of information regarding what their customers need.[142] The rules should encourage diversity in the system, tailoring control systems to the electricity sector, and should include security certification. For example, the Department of Homeland Security introduced cybersecurity procurement language for control systems in the hope that a common procurement language would facilitate a common understanding of and improve the security of the entire system.[143]

Diversity in products, services, and technology strengthens the system by eliminating common weaknesses that result in cascading failures.[144] For example, if a system has one type of operating program for all the computers in their wholesale power purchase department, then one virus can shut down the entire department because of the lack of diversity. Entities that support the

---

[136] *Hearing on H.R. 2195*, *supra* note 18, at 37.

[137] *See id*.

[138] *Id*. at 27, 29.

[139] Amoroso, *supra* note 45, at 190–92; *Hearing on H.R. 2195*, *supra* note 18, at 57.

[140] AMOROSO, *supra* note 45, at 192.

[141] *Id*. at 176.

[142] *Hearing on H.R. 2195*, *supra* note 18, at 20, 27.

[143] DEP'T OF HOMELAND SEC., CYBER SECURITY PROCUREMENT LANGUAGE FOR CONTROL SYSTEM (2008), *available at* http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf.

[144] AMOROSO, *supra* note 45, at 87. As part of a mid-term action plan for cybersecurity in general, the White House suggested refining "government procurement strategies and improv[ing] the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services." WHITE HOUSE CYBERSPACE POLICY REVIEW, *supra* note 118, at 38 (Table 3: Mid-Term Action Plan).

power grid would create a procurement and supplier management program, to maintain asset diversity. This may be difficult because it is contrary to the cost-saving industry practice of minimizing diversity, but the industry must commit to and invest in diversity.[145]

Existing procurement guidelines for critical infrastructure control systems could be tailored for the needs of the electricity sector.[146] For example, vendors can build systems such as firewalls for specialized SCADA environments and offer even more specialized products for substations and transmission components.[147] Another example is the requirement to include network-based security in contracts with Internet service providers.

A security certification program would verify and ensure an inherent baseline level of security. The certification program would be offered by a third party that tests independent technology and services. The results would give vendors a way to differentiate their products.[148] The control systems industry has procurement guides already and they could be modified for enhancing cybersecurity of the electric grid.[149]

D. Emergency Powers

In emergency situations, it is necessary for utilities to act quickly. In such a situation, investigating cyber events involves unpredictable legal and technical

---

[145] *Id*. at 72.

[146] *Hearing on H.R. 2195*, *supra* note 18, at 20.

[147] AMOROSO, *supra* note 45, at 72.

[148] *Hearing on H.R. 2195*, *supra* note 18, at 28. FEMA created the Private Sector Preparedness Accreditation and Certification Program ("PS-Prep"). According to designated standards, an independent board reviews private business preparedness for natural disasters, emergencies and business continuity. Certification can provide product differentiation. Perhaps insurance companies may offer lower rates to businesses that received certification through PS-Prep. *See generally The Voluntary Private Sector Preparedness Program*, FED. EMERGENCY MGMT. AGENCY, http://www.fema.gov/ps-preptm-voluntary-private-sector-preparedness (last visited May 1, 2013); Todd Keil, Assistant Sec'y for Infrastructure Prot., Dep't of Homeland Sec., Speech at the Critical Infrastructure Symposium (Apr. 29, 2011) [hereinafter Keil Speech].

[149] Consider NIST's smart grid cybersecurity strategy. NIST is working with vendors according to smart grid standards. The smart grid cybersecurity strategy will consist of an overall cybersecurity architecture to address points of failure, conformity assessment procedures, and certification criteria for personnel and processes. One concern is that legacy equipment might be difficult to modify to meet new standards. To ensure interoperability, products and systems will undergo conformity assessments developed by NIST. Once a standard has been published, vendors will have well-defined criteria to meet. Testing should ensure that cybersecurity standards do not interfere with cybersecurity. *Hearing on H.R. 2195*, *supra* note 18, at 67.

questions that may take more time than available.[150] The federal government with broad analysis of the national system may have a better sense of the appropriate response. Furthermore, it has the legal resources to examine the civil liberties issues and other legal liabilities that might be triggered by the utility's actions.[151] Allowing the federal government to have emergency powers to address immediate and pending threats would utilize its strengths.[152] It would ensure that the measures taken to mitigate imminent threats fit into the national or regional situation. For instance, an emergency directive could be the order for certain control systems to disconnect from the Internet and go to backup systems.[153]

There is general agreement among government and industry that a federal agency should have emergency powers.[154] There are situations that require federal government directed mandatory protective actions when the problems are widespread across state lines or national security is at risk.[155] FERC is often identified as the agency to hold these emergency powers.[156] FERC is the natural choice because it is the agency with the most expertise on the electric grid.[157] FERC has oversight of the bulk power system, but not over cybersecurity of the United States as a whole.[158] Its current responsibilities require it to review and comment on NERC cybersecurity standards.[159] Part IV, below, examines NERC standards in detail.[160]

Emergency powers must come with supporting mandates. FERC and any of

---

[150] *Id*. at 21, 26, 28.

[151] *See supra* notes 84–94 and accompanying text.

[152] *Hearing on H.R. 2195*, *supra* note 18, at 21, 26.

[153] AMOROSO, *supra* note 45, at 71. China's systems are considered strong from a defense perspective because the government can disconnect the power grid from the Internet. CLARK & KNAKE, *supra* note 45, at 187.

[154] *Hearing on H.R. 2195*, *supra* note 18, at 29, 47. In contrast, NERC believes that government emergency powers would decrease the effectiveness of private industry security responses because it would not act until government orders come through. David Perera, *NERC: Government In Electric Grid Controls 'Scary' to Contemplate*, FIERCEGOVERNMENTIT.COM (Feb. 13, 2011) http://www.fiercegovernmentit.com/story/nerc-government-intervention-electric-grid-controls-scary-contemplate/2011-02-13.

[155] *Hearing on H.R. 2195*, *supra* note 18, at 53.

[156] *Id*.

[157] *Id*. at 5. The National Association of Regulatory Utility Commissioners believes that FERC should be the government agency directing the energy sector during emergencies. *Id*. at 88. The proposed laws include provisions to give FERC emergency authority. *See infra* Part V. Some believe that FERC already has emergency authority. Weatherford Interview, *supra* note 133.

[158] 16 U.S.C. § 824*o* (2006).

[159] *Id*.

[160] *See* Part IV *infra*.

the entities involved in protecting the grid should not disclose sensitive information acquired or developed pursuant to the emergency power.[161] Before issuing an emergency order, FERC should consult with the appropriate industry experts to ensure that the order will not negatively affect grid operations.[162] It is suggested that emergency orders are appropriate only in national security events.[163] Finally, there must be cost recovery mechanisms associated with the emergency orders, as it is wise to ensure that emergency compliance measures will not cause financial harm.[164]

Emergency powers should apply to both transmission and distribution. Section 215 of the Federal Power Act gives FERC jurisdiction over transmission facilities, the "bulk power system," but FERC has not exercised any jurisdiction over local distribution facilities.[165] This means distribution systems for large cities like San Francisco, Chicago, and Boston will not have to comply with FERC emergency orders. The emergency powers should extend to metropolitan areas because of their impact on the larger regional systems. FERC could create guidelines for utilities that serve large cities so that there is better coordination with federal agencies and bulk power system entities resulting in a clear standard of response and expectations among all stakeholders during emergency situations.

E. International Cooperation

The Internet is an undeniable part of the electric grid, especially with the

---

[161] *Securing the Modern Electrical Grid From Physical and Cyber Attacks: Hearing Before the H. Select Comm. on Homeland Security*, 111 Cong. 48 (2009) (statement of Joseph H. McClelland, Dir. Of Reliability, Fed. Energy Regulatory Comm'n)*; Securing the Modern Electrical Grid From Physical and Cyber Attacks: Hearing Before the H. Select Comm. on Homeland Security*, 111 Cong. 54 (2009) (statement of Patricia M. Hoffman, Acting. Assistant. Sec'y, Office of Elec. Delivery and Energy Reliability, Dept. of Energy).

[162] *Id.*

[163] *See Securing the Modern Electrical Grid From Physical and Cyber Attacks: Hearing Before the H. Select Comm. on Homeland Security.*, 111 Cong. 23 (2009) (statement of Michael J. Assante, Chief Sec. Officer, N. Am. Electric Reliability Corp.).

[164] *Securing the Modern Electrical Grid From Physical and Cyber Attacks: Hearing Before the H. Select Comm. on Homeland Security*, 111 Cong. 48 (2009) (statement of Joseph H. McClelland, Dir. Of Reliability, Fed. Energy Regulatory Comm'n)*; Securing the Modern Electrical Grid From Physical and Cyber Attacks: Hearing Before the H. Select Comm. on Homeland Security*, 111 Cong. 54 (2009) (statement of Patricia M. Hoffman, Acting. Asstistant. Sec'y, Office of Elec. Delivery and Energy Reliability, Dept. of Energy).

[164] *Id.*

[165] 16 U.S.C. § 824(b) (2006) (stating that FERC has jurisdiction over wholesale energy in interstate commerce and all facilities for such transmission, and states have jurisdiction over facilities in local distribution and sale of energy intrastate); *see also* 16 U.S.C. § 824*o* (2006).

implementation of smart grid technology. Smart meters use the Internet or wireless connections to enable two-way communications between the utility and the home.[166] With these connections come risks.[167] The Internet exists independently of organizational, geographical, and political borders. Consequently, it is immensely difficult to identify the geographical origin of a cyber attack, or the perpetrator. To further complicate the situation, the attack and the perpetrator could have originated from multiple locations.[168] The information can travel in routes without any consideration for geographic lines.[169] Thus, international involvement is required to improve cybersecurity. International cooperation is important to prevent escalation if a U.S. utility inadvertently launches a cyber attack via active defense measures. Proposed legislation in Congress governing cybersecurity authorizes the Secretary of State to engage in a dialogue with international partners concerning the full range of cybersecurity issues in order to enhance cybersecurity and combat cyber crime.[170]

Cybersecurity and cyber terrorism investigations could involve police and security groups from different cities, states, and countries.[171] Unsurprisingly, the United States already participates in international agreements for investigations and prosecutions of cyber crimes.[172] For example, mutual legal assistance treaties ("MLATs") are formal bilateral agreements.[173] The United States has MLATs, in criminal matters with nineteen countries to provide mutual assistance combating cyber crime.[174] Effective in 2004, the members of the Council of Europe, a multilateral cooperation group of forty-seven countries, signed the Convention on Cybercrime.[175] The Convention seeks to address computer and Internet crime in Europe by providing for harmonization

---

[166] Weatherford Presentation, *supra* note 7.

[167] *Id*.

[168] Burstein, *supra* note 68, at 176 (describing a denial of service attack originating from a network of compromised computers but controlled by a remote perpetrator).

[169] *Id*.

[170] Cybersecurity Act of 2012, S. 2105, 112th Cong. § 904.

[171] Burstein, *supra* note 68, at 203.

[172] Suleyman Ozeren, Superintendent, Police Academy Ankara Turkey, *Cyberterroism and International Cooperation: General Overview of the Available mechanisms to Facilitate an Overwhelming Task*, *in* CENTER FOR EXCELLENCE DEFENSE AGAINST TERRORISM, RESPONSE TO CYBER TERRORISM 76 (IOS Press, 2008).

[173] *Id*. at 75.

[174] *Id*. at 76.

[175] *Id*.; Council of Europe Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/cadreprincipal.htm (effective 2004). The United States ratified the Convention on Cybercrime in 2006. Council of Europe Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174 (2006).

of cybercrime regulation amongst its members.[176] The Convention seeks to make criminal investigations relating to computer systems more effective and to ease collection of electronic evidence.[177]

International agreements should advance three underlying goals: deterrence, legal cooperation, and technical cooperation.[178] First, if mutual extradition and prosecution remove jurisdictional barriers to investigation and conviction, then perpetrators will be deterred from committing the act. Second, the agreements should encourage legal enforcement agencies to cooperate in investigations and prosecutions. Third, technical cooperation should stem from the agreements and result in sharing data, notices of threats, best practices, and solutions. Taken together, international agreements on cybersecurity can be effective.

The three underlying goals would enhance cybersecurity of the U.S. electric grid, especially when threats come from abroad. Deterrence can be achieved if there is a history of well-publicized, strong, mutual extradition and prosecution by numerous countries.[179] Similarly, the international agreements could increase cooperation between law enforcement agencies to collect evidence, build a case, and share technical information. Federal agencies involved in the electricity industry such as FERC, the Department of Energy ("DOE"), and the Department of Homeland Security ("DHS"), should consider how current international agreements can be used to achieve these goals and consequently improve cybersecurity of the electric grid in the United States.

IV. MANDATORY CYBERSECURITY STANDARDS BY NERC

Although the previous discussions took place against the backdrop of cybersecurity characteristics and challenges in general, Parts IV and V look at the mandatory cybersecurity standards and the proposed laws for the electricity sector in particular. With oversight from FERC, NERC is the Electric Reliability Organization responsible for creating and enforcing reliability standards for the power grid in the United States.[180] The standards from NERC also apply in many of the provinces of Canada and in a small part of Mexico.[181] Since the electricity sector is among the only sectors with

[176] Ozeren, *supra* note 172, at 78.

[177] *Id*. at 78–79.

[178] *Id*. at 76.

[179] Burstein, *supra* note 68, at 179–81 (discussing the limitations of deterrence).

[180] 16 U.S.C. § 824*o* (2006).

[181] *See, e.g.*, N. AM. ELECTRIC RELIABILITY CORP., THREE YEAR ERO PERFORMANCE ASSESSMENT REPORT 5–6 (2009), *available at* http://www.nerc.com/files/NERC_3-year_Assessment_report_7-01-09.pdf;

Canadian MOUs, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/FilingsOrders/ca/Pages/Canadian-MOUs.aspx (last visited June 15, 2013).

mandatory cybersecurity standards, it is a good starting point to examine the five components.[182]

Cybersecurity standards are a subset of the mandatory reliability standards, and any violation of the standards can result in fines of up to a million dollars per day.[183] This Part first gives a short description of the standards, and then analyzes them according to the five components of the recommended policy. Although the standards do not have all five components, they encourage information sharing. They offer opportunities for procurement rules and creating a foundation for adequate responses to government directives. The standards are naturally international as they are accepted in certain areas of Canada and Mexico,[184] but this is more based on the physical line connections in North America than a conscious effort to address cyber threats that cross international borders.

A. NERC Standards

The standards development process includes public notice and comment from a wide variety of stakeholders.[185] Stakeholders include not only generators and transmissions owners, but in addition, contractors and service providers of these grid entities participate.[186] The standards do not apply to all standards development participants, but rather only to "registered entities" ("REs") that perform power grid functions, such as reliability coordinators, transmission operators, and transmission planners.[187]

The electricity industry has been working on cybersecurity standards since the 1980s, but the 2003 East Coast blackout, which included parts of Canada,

---

[182] *See supra* note 3 and accompanying text.

[183] 16 U.S.C. § 824*o* (2006). Section 1211 of the Energy Policy Act of 2005 amended Part II of the Federal Power Act, adding Section 215 on Electric Reliability. *See* Southwestern Power Administration, No. NP11-238-000, 140 FERC ¶ 61,048 (Fed. Energy Regulatory Comm'n July 19, 2012) (order on review of notice of penalty), *available at* http://www.ferc.gov/whats-new/comm-meet/2012/071912/E-5.pdf (stating that section 215 of the FPA authorizes the imposition of a monetary penalty against a federal agency for violation of a mandatory reliability standard); *see also* Tim Roxey, Manager of Critical Infrastructure Protection, N. Am. Electric Reliability Corp., Presentation at Critical Infrastructure Symposium (Apr. 30, 2011) (stating that most of the violations this year will be cybersecurity standards violations).

[184] *See supra* note 181.

[185] N. AM. ELECTRIC RELIABILITY CORP., RELIABILITY STANDARDS DEVELOPMENT PROCEDURE 39–41 (2007), *available at* http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

[186] *Id.*

[187] N. AM. ELECTRIC RELIABILITY CORP., STATEMENT OF COMPLIANCE REGISTRY CRITERIA 2 (rev. 5.0, 2008), *available at* http://www.nerc.com/files/Statement_Compliance_Registry_Criteria-V5-0.pdf.

"was the first blackout in which software and information technology system failures were a major contributing factor."[188] The standards became mandatory when FERC approved them in 2008, along with a long list of required revisions.[189] FERC believed it was important to have the cybersecurity standards in place as soon as possible, even if revisions should be made.[190] This Part will discuss the standards in force today. It is not necessary to discuss the ongoing revisions themselves because the topics and goals of the standards remain the same.[191] The eight cybersecurity standards are part of the Critical Infrastructure Protection ("CIP") group and they cover the following topics relating to software and computer systems:

CIP-002: Critical Cyber Asset Identification,

CIP-003: Security Management Controls,

CIP-004: Personnel and Training,

CIP-005: Electronic Security Perimeters,

CIP-006: Physical Security,

CIP-007: Systems Security Management,

CIP-008: Incident Reporting and Response Planning, and

CIP-009: Recovery Plans for Critical Cyber Assets.[192]

The goal of CIP-002 (Critical Cyber Asset Identification) is to prioritize assets for protection by first identifying critical assets, and then from that list, identifying the critical *cyber* assets essential to the operation of the critical

[188] FERC APPROPRIATION 2004, *supra* 28; Roxey, *supra* note 183.

[189] Mandatory Reliability Standards for Critical Infrastructure Protection, 72 Fed. Reg. 16,461 (Mar. 16, 2007) (to be codified at 18 C.F.R. pt. 40).

[190] *See generally id.*

[191] FERC approved Version 4 of CIP-002 though CIP-009 on April 19, 2012 and the standards became effective on June 25, 2012. Currently under review are 10 CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), collectively referred to as the Version 5 CIP standards. *Cyber Security Order 706 Version 5 CIP Standards*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html (last visited Oct. 23, 2012).

[192] *See CIP Standards*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (last visited June 16, 2013). Version 4 establishes bright-line criteria for the identification of critical assets. *Id.* FERC approved version four of CIP-002 through CIP-009 on April 19, 2012 and the standards became effective on June 25, 2012. Version 4 Critical Infrastructure Protection Reliability Standards, 77 Fed. Reg. 24,594 (Apr. 25, 2012). FERC proposed a revised version of Critical Infrastructure Protection standards on April 18, 2013. Version 5 Critical Infrastructure Protection Reliability Standards, No. RM13-5-000, 143 FERC ¶ 61,055 (Fed. Energy Regulatory Comm'n Apr. 18, 2013) (notice of proposed rulemaking) (proposing to approve Version 5 of Critical Infrastructure Protection Reliability Standards, CIP-002-5 through CIP-011-1).

asset.[193] The REs use risk assessments to examine assets such as control centers and substations.[194] For example, after identifying a control center as a critical asset, the risk assessment determines that systems that manage real-time data exchange are critical cyber assets. The critical cyber assets list is important because it dictates to what assets the remaining seven standards apply.

Next, CIP-003 (Security Management Controls) requires the REs to create and implement a cybersecurity policy to protect information associated with critical cyber assets such as network diagrams and floor plans.[195] The policy must include a documentation process for changes, additions, modifications, and replacement of hardware or software.[196] The REs must document any inability to comply with their own policy and processes.[197]

Third, CIP-004 (Personnel Training) targets both the employee's access to sensitive assets and their cybersecurity knowledge and decision-making abilities.[198] The REs must screen personnel before granting access to critical cyber assets. The REs must maintain lists of people with unescorted physical access to critical cyber assets.[199] The training component of the standard is important for both existing employees and new employees to ensure that the most current protection methods are utilized.[200] This standard also addresses the undeniable human component of security; many security breaches occur simply because an employee gives out a password over the phone.[201] Training, posters, presentations, and meetings create an environment and culture of sound security practices with on-going reinforcement.[202]

---

[193] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-002-4: CYBER SECURITY—CRITICAL CYBER ASSET IDENTIFICATION (2011) [hereinafter CIP-002-4], *available at* http://www.nerc.com/files/CIP-002-4.pdf.

[194] *Id.*

[195] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-003-4: CYBER SECURITY—SECURITY MANAGEMENT CONTROLS (2011) [hereinafter CIP-003-4], *available at* http://www.nerc.com/files/CIP-003-4.pdf.

[196] *Id.*

[197] *Id.*

[198] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-004-4: CYBER SECURITY—PERSONNEL TRAINING (2011) [hereinafter CIP-004-4], *available at* http://www.nerc.com/files/CIP-004-4.pdf.

[199] *Id.*

[200] *Id.*

[201] AMOROSO, *supra* note 45, at 132–33; *see also* NAT'L ASS. OF STATE ENERGY OFFICIALS, SMART GRID & CYBER SECURITY FOR ENERGY ASSURANCE 21 (2010) (stating that cybersecurity must address the human element of cybersecurity, such as an insider threat, social engineering, and consumer behavior).

[202] CIP-004-4, *supra* note 198.

CIP-005 (Electronic Security Perimeters) and CIP-006 (Physical Security) protect cyber assets from unauthorized intrusions with electronic and physical tools.[203] The REs control access to critical assets via monitoring devices to detect and alert personnel of attempted or actual unauthorized access.[204] The REs must conduct an annual vulnerability assessment, including a review of passwords and network management.[205] Physical security protects the physical perimeter in which equipment is located by restricting physical access with card keys or special locks.[206] The REs monitor physical security with access logs and tests physical security mechanisms every three years.

CIP-007 (Systems Security Management) requires maintenance of the security system as a whole.[207] For example, new controls must be compatible with existing cybersecurity controls.[208] Security system maintenance requires monitoring by identifying incidents with automated or manual alerts, utilizing malicious software prevention tools, and documenting security patches.[209] The combined documentation for these activities can be analyzed to determine a correlation between certain indicators and cybersecurity threats. Unlike CIP-003 (Security Management Controls), which requires an overall cybersecurity policy, CIP-007 focuses on coordinating interactions between the users, legacy security systems, and new programs, so that the entire security system remains strong.

After preparing a cybersecurity policy and determining the electronic and physical security measures, the last two standards address reporting and recovery. CIP-003 (Security Management Controls) already requires the REs to create a response plan that includes incident classification and the response process.[210] CIP-008 (Incident Reporting and Response Planning) requires the REs to report the incident to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).[211] Since 1998, even before NERC became the

---

[203] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-005-4: CYBER SECURITY—ELECTRONIC SECURITY PERIMETERS (2011) [hereinafter CIP-005-4], *available at* http://www.nerc.com/files/CIP-005-4a.pdf; N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-006-4: CYBER SECURITY—PHYSICAL SECURITY (2011) [hereinafter CIP-006-4] *available at* http://www.nerc.com/files/CIP-006-4c.pdf.

[204] CIP-005-4, *supra* note 203.

[205] *Id*.

[206] CIP-006-4, *supra* note 203.

[207] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-007-4: CYBER SECURITY—SYSTEMS SECURITY MANAGEMENT (2011), *available at* http://www.nerc.com/files/CIP-007-4.pdf.

[208] *Id*.

[209] *Id*.

[210] CIP-003-4, *supra* note 195.

[211] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-008-4: CYBER SECURITY—

standard setting arm of FERC, NERC managed the ES-ISAC.[212] The ES-ISAC uses the industry's reports to post advisories and alerts, and determine the threat levels for the electricity sector.[213] As discussed in Part II, above, the ES-ISAC is an immature system and NERC is working to improve it to its full potential.

Lastly, CIP-009 (Recovery Plans for Critical Cyber Assets) requires a recovery plan, the goal of which is to ensure the least possible impact and interruption on system performance.[214] The plan must include accepted business continuity and disaster recovery techniques.[215] It should contain a variety of responses that will address the wide range of threats in duration and severity.[216] The plan should be carried out in practice and updated to reflect lessons learned from actual incidents or new information.[217]

B. NERC Standards Address Four of the Five Components.

The NERC cybersecurity standards create a foundation of sound security practices to defend the electric grid from cybersecurity threats. However, the NERC standards are not designed to address the worst-case scenario of "imminent threats."[218] Instead, they provide guidance as to the electricity sector's level of responsibility for cybersecurity and information sharing. The standards offer more opportunities to support procurement rules and emergency activities, but they have limited applicability in international cooperation.

INCIDENT REPORTING AND RESPONSE PLANNING (2011) [hereinafter CIP-008-4], *available at* http://www.nerc.com/files/CIP-008-4.pdf.

[212] N. AM. ELECTRIC RELIABILITY CORP., POLICY ON THE ROLE OF THE ELECTRICITY SECTOR—INFORMATION SHARING AND ANALYSIS CENTER (ES-ISAC) VIS-À-VIS NERC'S COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM 1 (2013) [hereinafter POLICY ON THE ROLE OF THE ELECTRICITY SECTOR].

[213] *Id*; Electricity Sector Information Sharing and Analysis Center, ES-ISAC, http://www.esisac.com/SitePages/Home.aspx (last visited, July 1, 2013) (stating that the ES-ISAC distributes "threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.").

[214] N. AM. ELECTRIC RELIABILITY CORP., STANDARD CIP-009-4: CYBER SECURITY—RECOVERY PLANS FOR CRITICAL CYBER ASSETS (2011), *available at* http://www.nerc.com/files/CIP-009-4.pdf.

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] *Hearing on H.R. 2195*, *supra* note 18, at 25.

1. NERC provides some assistance to clarifying the scope of responsibility.

The cybersecurity standards raise two conflicting issues with respect to the electricity industry's sense of responsibility. On one hand, CIP-002 (Critical Cyber Asset Identification), CIP-003 (Security Management Controls), and CIP-004 (Personnel and Training) indicate that the industry has responsibility for at least implementing a baseline cybersecurity program. However, there is confusion as to which assets should be deemed critical. On the other hand, the standards do not help the industry identify which agency is the lead agency in an emergency. This lead agency issue is a policy component separate from the scope of responsibility issue, but it should be highlighted here because the two issues overlap.

CIP-002 (Critical Cyber Asset Identification) is the basis for the other seven standards because it is impossible to create and implement a cybersecurity policy program without knowing the target of protection.[219] NERC discovered that only twenty-nine percent of generation owners and operators and sixty-three percent of transmission owners identified any critical assets. It is implausible that the electric grid has so few critical assets and the failure to identify critical assets leads to the failure to identify critical *cyber* assets.[220] CIP-002, version four, focuses on the functions supported by cyber systems and contains bright line rules for identifying critical assets. After the basic asset identification problem is resolved, the poor understanding of cybersecurity can be improved by each RE's cybersecurity policy, required by CIP-003 (Security Management Controls), and employee education, set forth in CIP-004 (Personnel and Training). Although NERC and some large entities acknowledge that the utilities should go beyond the baseline cybersecurity program to consider the worst-case scenario, the most worrisome entities are the small utilities with fewer resources.[221] Any entity, regardless of size, can be the weakest link in the electric grid security chain. Therefore, it is important that every entity recognizes its responsibility for the worst-case scenario. Such recognition does not necessarily mean spending money on consultants or installing new software. A company can reexamine the existing programs in the context of the entire industry and evaluate their effect on a holistic level.[222]

NERC is taking a proactive role in helping the industry with compliance and receiving feedback on its programs. For example, it issued guidelines about

[219] CIP-002-4, *supra* note 193.

[220] *See* Letter from Michael Assante, *supra* note 39.

[221] Susong Presentation, *supra* note 84 (stating that PG&E considers terrorist attacks in its cybersecurity policy); Weatherford Interview, *supra* note 133.

[222] Lee Presentation, *supra* note 122.

how the industry can address the vulnerability identified in the Aurora experiment.[223] The pilot Cyber Risk Preparedness Assessment is a partnership between NERC and industry that uses technical threat scenarios to assess how grid entities detect and mitigate the threats.[224] NERC has even hired contractors to test for vulnerabilities.[225] NERC conducted GRID EX in 2011, a cybersecurity incident readiness exercise that tested the electric industry's crisis response plans and allowed participants to respond to scenario events.[226]

The second issue applies to more than just the electricity sector, although NERC standards highlight cybersecurity challenges. Part of the scope of responsibility issue has to do with the confusion over who is the lead if there is a wide spread emergency situation. While the emergency powers issue will be discussed separately below, it is discussed in this Part because NERC is one of the main entities that should participate in determining and communicating to the industry the identity of the lead agency. Although the standards may not be the appropriate place to identify the lead agency, the private industry and governing entities, such as NERC, should know at least which agency to go to for assistance if there is an emergency.

Beyond FERC, DHS is supposed to be the lead agency for cybersecurity. It is responsible for the overall cybersecurity of the country and DHS leaders state that DHS is responsible for ".gov or .com" issues.[227] Its leadership position however is not always obvious because of other agencies do similar work. Another government lead is the U.S. Cyber Command, which is responsible for the Department of Defense. However, there may be situations

---

[223] *NERC Issues AURORA Vulnerability Guidelines*, *supra* note 51.

[224] N. AM. ELECTRIC RELIABILITY CORP., CYBER RISK PREPAREDNESS ASSESSMENT 3 (2011), *available at* http://www.esisac.com/Public%20Library/Reports/CRPA%20Program%202011%20Report.pdf.

[225] Siobhan Gorman, *Electricity Industry to Scan Grid for Spies*, WALL ST. J., June 18, 2009, http://online.wsj.com/article/SB124528065956425189.html.

[226] N. AM. ELECTRIC RELIABILITY CORP., 2011 NERC GRID SECURITY EXERCISE: AFTER ACTION REPORT 1 (2012), *available at* http://www.nerc.com/files/NERC_GridEx_AAR_16Mar2012_Final.pdf.

[227] Keil Speech, *supra* note 148; Weatherford Interview, *supra* note 133. While DHS has the responsibility for domestic defense and DOD for non-domestic issues, the National Security Agency has been trying to become more involved in cybersecurity. Many are uncomfortable with the potential liability implicated by sharing information with the government that may result in criminal prosecution and "inviting the shift from civilian to military control of government cybersecurity efforts aimed at the private sector." *Information Sharing, Monitoring, and Countermeasures in the Cybersecurity Act, S. 2105 and the SECURE IT Act, S. 2151*, CTR. FOR DEMOCRACY & TECH. (Mar. 28, 2012), https://www.cdt.org/files/pdfs/analysis_senate_cyberbills_2012.pdf. Focus should be less on cyberweapons and more on international police cooperation and treaties. Bruce Schneier, *supra* note 49.

where this assistance extends to the private industries in the critical infrastructure sectors.[228] The difficulty with attribution exacerbates the problem because such information affects whether DHS or the U.S. Cyber Command is responsible and involved.[229] The simple fact is that the confusion over federal agency leadership in times of emergency or extreme situations diminishes the strength of critical infrastructure when it is needed the most. Clear leadership must be identified and it must be communicated to the industry.[230]

2. NERC's ES-ISAC is one of the many information outlets.

NERC's ES-ISAC gathers information from the electricity sector, analyzes it, and posts advisories and warnings on its website.[231] The ES-ISAC provides a reliable source of information from the industry because NERC standard CIP-008 (Incident Reporting and Response Plan) requires reporting to the ES-ISAC.[232] While this is helpful, the ES-ISAC is only one of many information collectors.[233] The DOE and DHS have their own information gathering mechanisms.[234] A national situational awareness program could compile data from both private and government sources, yet at this time a national-level information aggregator and analysis center for the electric grid does not exist.

NERC has coordinated the ES-ISAC since the late 1990s, but it is specific to the electricity industry and gathers information reported by the industry.[235] To explore alternative avenues, NERC created other information/communication initiatives such as the voluntary alert system to distribute information about vulnerabilities or attacks identified by NERC or by other government agencies.[236] The alerts reach almost 5,000 electric grid professionals and NERC has received positive comments from the industry.[237]

The DOE gathers energy sector-specific information by requiring the electricity industry to file Form EO-417, Electric Emergency Incident and Disturbance Report, for emergency incidents such as cyber disturbances.[238]

---

[228] CLARK & KNAKE, *supra* note 45, at 140.

[229] Susong Presentation, *supra* note 84 (stating that when there is not enough information to categorize a cyber event as a security breach or attack, it is unclear which federal agency is the lead).

[230] Weatherford Interview, *supra* note 133.

[231] POLICY ON THE ROLE OF THE ELECTRICITY SECTOR, *supra* note 212, at 1.

[232] *Id.*; CIP-008-4, *supra* note 211.

[233] *See infra* notes 239–247 and accompanying text.

[234] POLICY ON THE ROLE OF THE ELECTRICITY SECTOR, *supra* note 212, at 1.

[235] *Id.*

[236] *Hearing on H.R. 2195*, *supra* note 18, at 26.

[237] *Id.*

[238] Office of Electricity Delivery and Energy Reliability, *Electric Disturbance Events*

DOE uses the information to create situational awareness of the U.S. electricity grid.[239] The DOE Energy Information Administration ("EIA") publishes the electric power emergency incidents and disturbances in its monthly EIA reports.[240] DOE shares data with FERC when appropriate.[241]

Unlike the DOE, the DHS receives intelligence information not just from the electric sector, but also from other critical infrastructure sectors.[242] DHS's Control System Security Program evaluates cybersecurity operational risk management, and "develops mitigation plans to manage risk to an acceptable level."[243] The DHS Homeland Security Infrastructure Threat and Risk Analysis Center ("HITRAC") develops early intelligence warnings, which it shares with the DOE and DOD.[244] Another DHS office, US-CERT, provides response support and defense against cyber attacks on the federal civil executive branch.[245] When possible, the information it gathers from the government is shared with state and local government, industry, and international partners.[246]

Ideally, all unredacted government information from DHS, DOE, and industry should go to a central repository on a guaranteed and consistent basis. Several programs attempt to create a public/private data and analysis center. The Protected Critical Infrastructure Information Program ("PCII") at DHS

(OE-417), DEPT. OF ENERGY (July, 2012), http://www.oe.netl.doe.gov/oe417.aspx; DEPT. OF ENERGY, ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT (2012) [hereinafter DOE INCIDENT REPORT], *available at* https://rfirst.org/compliance/Documents/DOE%20Form%20OE-417%20Instructions.pdf

[239] DOE INCIDENT REPORT, *supra* note 238, at 1 (explaining that the DOE uses the information for analytical purposes).

[240] *Id*.

[241] *Hearing on H.R. 2195*, *supra* note 18, at 57.

[242] *Id*. at 62; DEPT. OF HOMELAND SEC., ICS-CERT MONITOR (Jan.–Mar., 2013), *available at* https://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_Jan-Mar2013.pdf (stating it works with all critical infrastructure sectors in almost all states).

[243] *Hearing on H.R. 2195*, *supra* note 18, at 62.

[244] *See* DEPT. OF ENERGY AND DEPT. OF HOMELAND SEC., ENERGY: CRITICAL INFRASTRUCTURE RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (REDACTED) 32-33 (2007), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_Public.pdf.; DEPT. OF HOMELAND SECURITY, DEPT. OF ENERGY, ENERGY SECTOR-SPECIFIC PLAN, AN ANNEX TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN 36 (2010) *available at* www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf (stating one of the products provided by HITRAC is to brief representatives from the Intelligence Community, including DHS, DOD, and DOE).

[245] *About Us*, US-CERT.GOV, http://www.us-cert.gov/about-us (last visited May 1, 2013).

[246] *Id*.

allows the private sector to voluntarily share information with DHS despite state and federal disclosure laws.[247] Similarly, NERC sponsors Network HYDRA, a network of subject matter experts who identify, analyze, and share information on electric grid vulnerabilities.[248] It also works with industry, DOE, and DHS, almost on a daily basis to provide better information on threats and cyber activity.[249] Still, participation in these information-sharing partnerships is voluntary and inconsistent.

Therefore, there are many organizations working on similar issues without a lead agency or organization to coordinate the efforts or serve as a central repository. The repository would guarantee a complete national-level situational awareness, as opposed to one with gaps as government and private data are distributed among different organizations. DOE may be the appropriate lead agency and/or repository because it already gathers information to create situational awareness updates for the grid. It also has authority to collaborate with federal agencies, state and local government, and the private sector to conduct vulnerability assessments and encourage risk management.[250] Without such a center, the industry is in the precarious and time-consuming position of trying to analyze incomplete information itself.

3. Procurement rules can be part of NERC cybersecurity standards.

Vendors can and should build security into their products. In general, the demand has not reached the point where vendors are forced to offer products with better security characteristics. Often, products with better cybersecurity are more expensive without providing obvious improvements in daily performance.[251] If the cybersecurity protection works, then the system will operate as usual and it is hard to assign a monetary value on the avoided impacts. For the electricity sector, NERC mandatory standards create value in compliance and the avoidance of fines and legal fees. The regulated entity can avoid costs if the assets were already designed with security measures. While procurement rules and guidelines can be voluntary or mandatory, the mandatory NERC standards can be revised to incorporate vendor evaluations.[252]

---

[247] *Protected Critical Infrastructure Information Program*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/editorial_0404.shtm (last visited May 1, 2013).

[248] *Hearing on H.R. 2195*, *see supra* note 18, at 23.

[249] *Id*. at 25, 45 (stating that NERC collaborating with DOE and DHS to provide situational awareness of threats and suspicious activities).

[250] *Id*. at 57.

[251] Burstein, *supra* note 68, at 171, 177 ("[T]he current culture of security encourages individuals and institutions to view security as an expense rather than a necessary means of avoiding lost time, money, and information.").

[252] *Hearing on H.R. 2195*, *supra* note 18, at 13, 18.

Like the current standards, which aim to establish a baseline cybersecurity program, the procurement requirements should establish a baseline upon which the REs can build their policies and programs. The procurement requirements should encourage two things. First, the products' cybersecurity characteristics should be tailored to the electricity sector. For example, firewalls should address SCADA systems and grid components like transmission facilities and substations. Second, the procurement requirements should put the vendors on notice that a certain level of diversity in products and services is necessary to prevent cascading failures.

If the procurement rules were mandatory, then revisions to CIP-003 (Security Management Controls), CIP-005 and CIP-006 on the electronic and physical security perimeters, and CIP-007 (System Security Management) could incorporate vendor evaluations.[253] For example, the cybersecurity policy in CIP-003 (Security Management Controls) could include a procurement and supplier management program that evaluates vendors and ensures diversity. CIP-005 and CIP-006 on electronic and physical controls could be even more specific. They could require the REs to evaluate the vendors' products for cybersecurity characteristics, such as the level of protection against someone hacking into a key card system. CIP-007 could ask the REs to examine whether the new products provide more assurances that their installation or implementation will not weaken existing cybersecurity measures.

A third-party security certification program for electricity industry products could support the mandatory standards. The standards would create the demand and value for certified products and vendors would have a way to distinguish themselves. NERC could play a supporting role in creating the certification program via stakeholder meetings, identifying measures, and providing examples from existing certification programs in other industries.

4. NERC standards do not address emergency powers.

Federal emergency powers are necessary to guide the industry's response in situations that cross state lines, or that are so serious as to compromise national security. As noted in the Part III.A, it is unclear who will take the lead in emergency situations when there are imminent threats. As discussed below in Part V on proposed laws, FERC is prepared to exercise the emergency power.[254] NERC has a role, albeit indirectly.

The CIP standards set basic security practices to create a foundation against cybersecurity threats, but they are not designed to address worst-case scenarios such as coordinated cyber attacks. As the standard-setting entity, NERC defers

[253] *Id*. at 32 (stating that NERC standards in action actually improves security).

[254] Weatherford Interview, *supra* note 133 (stating that FERC determines the threats while NERC determines the vulnerabilities).

to FERC on the overall policy of the electricity sector. [255] Nevertheless, two NERC standards affect emergency powers. First, CIP-008 (Incident Reporting) helps the responsible federal agency gather information on the threats and the remediation measures. Second, when complying with CIP-009 (Recovery Plans), the registered entities should create plans flexible enough to incorporate emergency orders. These two standards encourage planning for the implementation of any specific guidance that may accompany emergency orders on fixing the vulnerabilities related to a specific threat.

5. NERC's international activities

NERC's standards are mandatory in the United States and they apply in Canada and Mexico on a more limited base. Indeed, NERC standards are naturally international because the North American continental grid connects the United States to Canada and Mexico. However, this limited international character does not address the more expansive international reach of cyber threats. NERC, while aware of these issues, does not actively participate in international law and policy development.[256] Admittedly, NERC may not have the resources to help the international community with cybersecurity policy, but it can disseminate educational materials to the U.S. electric industry on topics such as applicable international law, extradition, and prosecution.

* * * * *

After evaluating the mandatory NERC standards according to the five policy components, NERC standards show that with some changes, it is not far from providing a comprehensive cybersecurity policy for the electricity grid. Perhaps NERC's role as a standard setting entity caused it to contribute more to the first four components. It contributes to the industry's understanding of its responsibilities by requiring a basic cybersecurity program. The NERC ES-ISAC also helps with information sharing. There are opportunities for using the NERC standards to create procurement requirements. Furthermore, NERC standards could support emergency directives as well. NERC, however, does not contribute to international cooperation, but it can give international agreements legitimacy by supporting them. Several proposed laws try to address some of the issues that NERC does not, but as discussed in the next Part, both regulatory and legal changes are needed to satisfy the five policy components.

[255] *See* John S. Moot, *When Should the FERC Defer to the NERC?*, 31 ENERGY L.J. 317, 332 (2010).

[256] Weatherford Interview, *supra* note 133.

V. PROPOSED LAWS

In response to the numerous reports of cyber attacks and the general public perception that the U.S. electric grid is vulnerable, Congress has considered several new laws in the last few years. The Bulk Power System Protection Act ("H.R. 2165") and the Critical Electric Infrastructure Protection Act ("H.R. 2195") were both introduced in 2009,[257] but neither passed the House of Representatives.[258] The Grid Reliability Infrastructure Defense Act ("H.R. 5026") passed the House in 2010, and it was placed on the Senate legislative calendar, but it did not progress any further.[259] All three proposals addressed, in one way or another, three parts of the comprehensive cybersecurity policy: the recognition of responsibility, information sharing, and emergency powers. However, the proposals did not address procurement rules and only addressed international cooperation tangentially.

A. H.R. 2165—The Bulk Power System Protection Act

H.R. 2165 would give FERC explicit authority to respond to imminent cybersecurity threats.[260] It referred to the term "bulk power system," as defined in Section 215 of the Federal Power Act,[261] which does not include lower voltage distribution lines.[262] As such, H.R. 2165 would require defense facilities with lower voltage lines in Alaska, Hawaii, and Territory of Guam to have their own emergency plan of measures or actions in the event of an imminent cyber threat because they are not part of the U.S. continental "bulk power system."[263] H.R. 2165 would require FERC to consult with the governments of Canada and Mexico to create, by rule or order, measures or

---

[257] *See* Bulk Power System Protection Act of 2009, H.R. 2165, 111th Cong. (2009); H.R. 2195, 111th Cong. (2009). H.R. 2195 is herein referred with the short title of its companion bill in the Senate. *See* Critical Electric Infrastructure Protection Act of 2009, S. 946, 111th Cong. § 1 (2009).

[258] Each bill "[d]ied" in committee. *See H.R. 2165*, GOVTRACK.US, http://www.govtrack.us/congress/bills/111/hr2165 (last visited June 18, 2013); *H.R. 2195*, GOVTRACK.US, http://www.govtrack.us/congress/bills/111/hr2195 (last visited June 18, 2013).

[259] Grid Reliability and Infrastructure Defense Act, H.R. 5026, 111th Cong. (2010); *THOMAS Bill Summary & Status H.R.5026*, LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR05026:@@@R (last visited June 18, 2013).

[260] H.R. 2165 § 1(a) (amending § 215A(b) of the Federal Power Act).

[261] *Id.* § 1(a) (amending § 215A(a) of the Federal Power Act).

[262] 16 U.S.C. § 824(b)(1) (2006) (stating that FERC has jurisdiction over wholesale of energy in interstate commerce and all facilities for such transmission and states have jurisdiction over facilities in local distribution and sale of energy intrastate); *see also* 16 U.S.C. § 824*o* (2006).

[263] H.R. 2165 § 1(a) (amending § 215A(c)(1) of the Federal Power Act).

actions that protected the bulk power system from cybersecurity threats.[264] Later on, these measures could become cybersecurity reliability standards by NERC.[265] Upon receiving a written directive from the President that an imminent cybersecurity threat existed, H.R. 2165 would allow FERC to order emergency measures or actions necessary to protect the grid from the threat within thirty days.[266] If appropriate for the threat and if time permits, FERC would consult with authorities in Canada and Mexico.[267] The emergency order would terminate by a FERC order, a Presidential order, or a subsequent reliability standard implemented to address the identified threat.[268] During the emergency event and the resulting directives or orders, appropriate sensitive information could be released to entities subject to the emergency orders for compliance purposes, but any disclosure must follow a confidentiality procedure.[269] Notably, H.R. 2165 would provide industry with government assistance. The assistance would include the development of resources, such as hardware, software and equipment, sharing expertise, and security clearance to industry personnel to allow for "optimum understanding of cybersecurity threats and ability to respond."[270] The bill did not proceed any further than referral to the House Subcommittee on Energy and Environment.[271]

B. H.R. 2195—The Critical Electric Infrastructure Protection Act

The Critical Electric Infrastructure Protection Act, H.R. 2195, would expand the roles of FERC and DHS. Unlike H.R. 2165, H.R. 2195 would cover the entire spectrum of electric facilities, from transmission, distribution, down to the meters.[272] This would include large cities' distribution facilities, such as those in Los Angeles, New York, and Washington, D.C. In addition to cyber threats of the computer virus variety, H.R. 2195 would apply to electromagnetic pulse ("EMP") events that could be intentional or natural.[273] These EMP events, including solar storms, can disrupt SCADA systems and melt transformers. DHS would assess cyber vulnerabilities and threats to the electric grid, perform ongoing tests, and recommend mitigation methods to

[264] *Id*. (amending § 215A(b)(1) of the Federal Power Act).

[265] *Id*. (amending § 215A(b)(2), (d)(3) of the Federal Power Act).

[266] *Id*. (amending § 215A(d), (e) of the Federal Power Act).

[267] *Id*. (amending § 215A(b)(1), (c)(2) of the Federal Power Act).

[268] *Id*. (amending § 215A(d), (e) of the Federal Power Act).

[269] *Id*. (amending § 215A(f) of the Federal Power Act).

[270] *Id*. (amending § 215A(j)(4) of the Federal Power Act).

[271] *H.R. 2165*, *supra* note 258.

[272] H.R. 2195, 111th Cong. § 1(c) (2009) (amending § 224(a)(1), (c) of the Federal Power Act).

[273] *See id*. § 1(a)(5).

FERC.[274] FERC would issue rules and orders on a routine basis to address identified vulnerabilities or threats.[275] FERC would have the option of using its emergency powers to address imminent threats.[276] Emergency rules or orders would be effective for less than ninety days subject to changes by FERC.[277] In consultation with DHS, FERC would be authorized to replace existing cybersecurity standards if it found that the existing standards were inadequate.[278] NERC could replace the FERC standards later. H.R. 2195 would protect information by applying Section 214 of the Critical Infrastructure Information Act of 2002.[279] Among other things, Section 214 would protect the disclosing parties' information and encourage such disclosures by exempting such information from the Freedom of Information Act and state and local disclosure laws.[280] H.R. 2195 was introduced in a previous session of Congress and was not enacted.[281]

C. H.R. 5026—The Grid Reliability Infrastructure Defense Act

In 2010, Representative Edward Markey introduced H.R. 5026.[282] After passing in the House, the Senate amended version of H.R. 5026 contained similar provisions from both H.R. 2165 and H.R. 2195.[283] Similar to H.R. 2195, "critical electric infrastructure" meant not only transmission assets, but also distribution assets.[284] Despite H.R. 5026's applicability to distribution, military defense facilities in Alaska, Hawaii, and Guam would be required to have their own emergency cyber threat response plans because they were not connected to the "bulk power system."[285] H.R. 5026 would allow FERC to use its emergency powers to issue rules or orders to protect critical electric infrastructure from cybersecurity vulnerabilities, and if possible, FERC would consult with industry and other Federal agencies.[286] Unlike the previous bills,

[274] *Id*. § 1(c) (amending § 224(b) of the Federal Power Act).

[275] *Id*. (amending § 224(c)(1) of the Federal Power Act).

[276] *Id*. (amending § 224(c)(2) of the Federal Power Act).

[277] *Id*. (amending § 224(d) of the Federal Power Act).

[278] *Id*. (amending § 224B of the Federal Power Act).

[279] *See Protected Critical Infrastructure Information Program*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/editorial_0404.shtm (last visited May 3, 2011).

[280] H.R. 2195 § 1(c) (amending § 224(f) of the Federal Power Act).

[281] *H.R. 2195*, *supra* note 258.

[282] Grid Reliability and Infrastructure Defense Act, H.R. 5026, 111th Cong. (2010); *THOMAS Bill Summary & Status H.R.5026*, LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR05026:@@@R (last visited June 18, 2013).

[283] *See* H.R. 5026 (as reported by S. Comm. on Energy and Natural Res., Sept. 27, 2010).

[284] *Id*. § 1 (amending § 224(a)(1) of the Federal Energy Act).

[285] *Id*. (amending § 224(f) of the Federal Energy Act).

[286] *Id*. (amending § 224(b) of the Federal Energy Act).

the Secretary of Energy would have the emergency powers to order entities under FERC's jurisdiction to take actions to mitigate cybersecurity threats.[287] What differentiated the Secretary of Energy's powers from FERC would be that before exercising his/her authority, the Secretary would be encouraged to coordinate with Canadian and Mexican officials, the industry, and other federal agencies.[288] Under H.R. 5026, the emergency rules or orders would expire within ninety days, by act of FERC, or on the date a NERC cybersecurity standard would become effective to address the identified vulnerability.[289] The bill would require FERC to develop a mechanism by which utilities could recover costs prudently incurred due to compliance with the emergency orders.[290] Lastly, like H.R. 2195, H.R. 5026 would use Section 214 of the Critical Infrastructure Information Act of 2002 to protect information compiled by FERC and DOE. FERC and DOE would create procedures to share the information after careful evaluation of purpose, confidentiality, and privacy.[291] H.R. 5026 passed the House, but did not progress through the Senate.[292]

D. The Proposed Laws Address Three out of the Five Components

All three bills addressed three out of the five components suggested in this Article—namely, the division of responsibility, information sharing, and emergency powers. The bills did not address procurement rules. Furthermore, they only mention incidentally international cooperation, since any collaboration with Canada and Mexico was due to their physical ties to the U.S. grid, and was not due to any directed effort to address the wide-ranging international effects of cyber threats.

1. The bills address responsibility in emergency situations

The proposed laws address the measures and actions that must be taken by the electric industry in the post-event period, after a threat has been identified or an emergency has been declared. They do not elaborate on the industry's pre-event responsibilities, meaning the preventative measures that should be in place already. The lawmakers may have believed that the NERC standards already addressed pre-event protective measures and decided to concentrate on post-event governance. The bills required that the industry has the capacity and resources to comply with emergency directives in the event the electric industry identified an emergency. The industry's responsibility to follow the

[287] *Id*. (amending § 224(c) of the Federal Energy Act).
[288] *Id*. (amending § 224(c)(2) of the Federal Energy Act).
[289] *Id*. (amending § 224(d) of the Federal Energy Act).
[290] *Id*. (amending § 224(c)(4) of the Federal Energy Act).
[291] *Id*. (amending § 224(g) of the Federal Energy Act).
[292] *THOMAS Bill Summary & Status H.R.5026*, *supra* note 282.

emergency directives continued after the threat was resolved because in all three bills the emergency orders can become mandatory reliability standards.[293] The bills differ slightly as to who would issue the emergency orders. All three identified FERC as a lead, but H.R. 2195 gave DHS a role in threat identification and analysis, and H.R. 5026 allowed the Secretary of Energy to issue emergency orders as well.[294] These proposals are an incremental step towards assignment of responsibility because they identify the leader and the role of the leader for the electricity sector.

2. The bills address information sharing and the controlled disclosure of information generated during emergency situations.

Information sharing could encourage better mitigation measures. More importantly, it can create a national-level situational awareness for both government and industry information. All bills made efforts to create more information sharing, but they lacked direction. In an opposite, albeit appropriate direction, there was a clear emphasis on protecting from disclosure information generated during the emergency.

The three bills contained different proposals on how to share information. H.R. 2165 mentioned government assistance through sharing classified information with industry.[295] H.R. 2195 directed DHS to analyze threats and vulnerabilities and to make mitigation recommendations to FERC.[296] If DHS identified a cyber threat to or vulnerability in the electricity system, DHS would communicate the information to FERC in a timely manner.[297] In H.R. 5026, FERC and DOE would share information.[298] These efforts are incomplete because each bill represents only one part of a comprehensive information sharing system. The ideal involves information sharing between industry, DHS, DOE, and FERC.[299] DHS would analyze threats and

[293] *See* H.R. 2165, 111th Cong. § 1(a) (2009) (amending § 215A(d)(3) of the Federal Power Act); H.R. 2195, 111th Cong. § 1(c) (2009) (amending § 224B(a)(2) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(b)(4) of the Federal Energy Act).

[294] *See* H.R. 2165 § 1(a) (amending § 215A(b) of the Federal Power Act); H.R. 2195 § 1(b), (c) (amending § 224B(a)(2) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(b), (c) of the Federal Energy Act).

[295] H.R. 2165 § 1(a) (amending § 215A(f) of the Federal Power Act).

[296] H.R. 2195 § 1(c) (amending § 224(b) of the Federal Power Act).

[297] *Id*.

[298] H.R. 2165 § 1(a) (amending § 215A(g) of the Federal Power Act).

[299] There are examples of collaboration. The *Roadmap to Secure Control System in the Energy Sector* is a ten year plan to secure critical infrastructure by the DOE, DHS, Natural Resources Canada and industry. The goal of the roadmap is, by 2016, control systems for critical infrastructure will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function. DOE is cost-sharing two projects

vulnerabilities, the results of which it would share with FERC and DOE, while DOE would create a national-level, real-time situational awareness.[300] The bills did not contain such a proposal to help the private sector anticipate threats more quickly and accurately.

All bills sought to protect information generated during the emergency period or pursuant to compliance with emergency orders. They required careful control over disclosure of information gathered during the emergency period. H.R. 2165 described the confidentiality procedures and the disclosure limitations as to sensitive cybersecurity information.[301] Both H.R. 2195 and H.R. 5026 referred to Section 214 of the Critical Infrastructure Information Act of 2002 and exempted certain information from disclosure.[302] H.R. 5026 incorporated part of H.R. 2165 by including a requirement to develop an information release procedure.[303] Preventing information from falling into the hands of the wrong entities improves overall security in the long term. Still, there was no proposal for a national-level data aggregator and analysis center, despite much language being devoted to protecting information. In general, this means there continues to be a deep reluctance to release information and there is still a lack of acceptance of information sharing today.

3. The bills did not address procurement rules.

Procurement rules that encourage vendors to provide products with cybersecurity built into the system were absent from the bills. The bills did not address the importance of diverse products or a cybersecurity certification program. This may be due to the fact that procurement rules are often

---

that are implementing the Roadmap. One project develops checklists of security configuration baselines that can enable the audit of actual configuration settings against these baselines and another project to commercialize the secure SCADA Communications Protocol. *See generally* U.S. DEP'T OF ENERGY, ROADMAP TO SECURE CONTROL SYSTEMS IN THE ENERGY SECTOR (2006), *available at* http://energy.gov/oe/downloads/roadmap-secure-control-systems-energy-sector-2006; U.S. DEP'T OF ENERGY, ROADMAP TO ACHIEVE ENERGY DELIVERY SYSTEMS CYBERSECURITY (2011), *available at* http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

[300] Currently, the DOE and the DHS have programs that test control systems technology for vendors and utilities under contract. Because of the contracts, the information belongs to the vendor or utilities and is not available to the public. *Hearing on H.R. 2195, supra* note 18, at 35. *See also* U.S. Computer Emergency Readiness Team, U.S. Dep't of Homeland Sec., *Control Systems Security Program (CSSP)*, ICS-CERT, http://www.us-cert.gov/control_systems/csfaq.html (last visited May 8, 2011).

[301] H.R. 2165 § 1(a) (amending § 215A(f) of the Federal Power Act).

[302] H.R. 2195 § 1(c) (amending § 224(f) of the Federal Power Act); H.R. 5026, 111th Cong. § 1 (2010 (amending § 224(g)(1) of the Federal Energy Act).

[303] H.R. 5026 § 1 (amending § 224(g) of the Federal Energy Act).

guidance and are not legally mandated.[304] As for the electricity sector in particular, Part IV, above, of this Article discussed how the NERC standards could support procurement rules that require vendors to provide a baseline security level and evaluation. Nevertheless, a legislative mandate could be helpful.

4. The bills focused on emergency powers.

The three proposed laws examined here focused on federal emergency powers, and those powers will likely be the focus of any future proposals. Both the electric industry and the federal government agree there must be a law in place to deal with imminent threats and emergencies.[305] The bills envisioned government directed responses for private industry. Usually, the bills named FERC as having emergency powers. In the most recent bill, FERC shared the authority with the Secretary of Energy.[306]

The bills grappled with the scope of FERC's jurisdiction over just the "bulk power system," which encompasses transmission but not distribution facilities. This could be harmful when distribution facilities of large cities have serious impacts on the grid overall. Hence, more explicit authority over systems beyond transmission would be beneficial. H.R. 5026 extended authority over systems beyond transmission to distribution, and better yet, H.R. 2195 reached metering equipment.[307] As discussed in the information sharing section, all bills were keen to protect sensitive information generated by an emergency situation.[308] Finally, the details varied as to when emergency provisions should be issued and when they should expire.[309] Yet, all bills provide for new mandatory reliability standards based on the emergency orders so that the same threats would not affect the grid in the future.[310]

---

[304] *See* DEP'T OF HOMELAND SEC., CYBER SECURITY PROCUREMENT LANGUAGE FOR CONTROL SYSTEM vii (2008), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf (presenting suggested language for industrial control systems procurement).

[305] *See generally Hearing on H.R. 2195*, *supra* note 18.

[306] H.R. 5026 § 1 (amending § 224(c) of the Federal Energy Act)

[307] *Compare id.* (amending § 224(a)(1) of the Federal Energy Act), *with* H.R. 2195 § 1(b) (amending § 224(a)(1) of the Federal Power Act).

[308] *See supra* Part V.D.2.

[309] H.R. 2165, 111th Cong. § 1(a) (2009) (amending § 215A(c), (e) of the Federal Power Act); H.R. 2195 § 1(b), (c) (amending § 224(d) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(b)(4), (d) of the Federal Energy Act).

[310] *See* H.R. 2165 § 1(a) (amending § 215A(d)(3), (e)(3) of the Federal Power Act); H.R. 2195 § 1(c), (d) (amending § 224(d) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(b)(4) of the Federal Energy Act).

5. The bills did not encourage international cooperation.

Disappointingly, none of the bills recognized or discussed the lack of political and geographic boundaries in cyber threats. Any international cooperation was limited to consulting with officials in Canada and Mexico because they are part of the North American electric grid, and they adopted the NERC reliability standards.[311] The bills relied on geographic and physical connections. Even though international-level activities outside North America affect cybersecurity of the electric grid, the bills failed to mention or promote deterrence, legal cooperation, and technical cooperation via international agreements.

* * * * *

Overall analysis of the bills according to the five components shows that the bills dealt with emergency powers in the post-event period. They did not speak to the responsibilities of the industry to install pre-event preventative cybersecurity measures. The bills indicated that the federal government should step in to give industry guidance in certain situations, although it was still nebulous as to the exact type of event and when. The bills proposed that the government fulfill its responsibility during these situations via its emergency powers, mainly assigned to FERC. The bills contained provisions that allowed sharing of information and collaboration, but no bill suggested one comprehensive program for national-level data gathering and analysis involving DHS, DOE, NERC, FERC, and the electric industry. H.R. 2195 gave DHS the responsibility of sharing analysis and recommendations with FERC, while H.R. 5026 provided for information sharing between DOE and FERC.[312] The only clear leader that the bills identified was FERC, but still they provided no clear leadership for cybersecurity overall. Finally, procurement rules were left out of the bills, as were international cooperation.

VI. CONCLUSION

Inevitably, media attention on smart grid deployment and the increase in automation and Internet connections highlight the complex cybersecurity vulnerabilities of the electric grid.[313] Continuing the focus from previous

[311] *See* H.R. 2165 § 1(a) (amending § 215A(b) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(c)(2), (3) of the Federal Energy Act).

[312] H.R. 2195 § 1(c), (d) (amending § 224(b) of the Federal Power Act); H.R. 5026 § 1 (amending § 224(g) of the Federal Energy Act).

[313] Meserve, *supra* note 37; Kim Zetter, *Maker of Smart-Grid Software Hacked*, WIRED.COM (Sept. 26, 2012, 3:56 pm), http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked/; *Cybersecurity: Plugging smart grid weakness*, PHYS.ORG, (June 5, 2013), http://phys.org/news/2013-06-cybersecurity-smart-grid-weaknesses.html.

administrations, President Barack Obama made cybersecurity a centerpiece of his policy goals.[314] Likewise, in Congress, there are many proposals that go beyond the electric grid to address critical infrastructure overall.[315] In the Cybersecurity Act of 2012, which President Obama supported, critical infrastructure is any system, if damaged, that could result in "interruption of life-sustaining services," "catastrophic economic damage," and "severe degradation of national security."[316] Ultimately, the Act did not pass the Senate,[317] but this and other efforts show that if cybersecurity is not addressed with electric industry-specific legislation, it will be part of a wider effort. In his State of the Union Address, President Obama emphasized his commitment to addressing cybersecurity threats to critical systems such as the power grid, financial institutions, and air traffic control systems, and he referenced an Executive Order improving critical infrastructure cybersecurity he had signed earlier that day.[318] Analysis of more expansive proposals is beyond the scope of this Article and will have to be the subject of further scholarship.

Initially, this Article presented the challenges of cybersecurity, such as planning and prediction difficulties, the attribution problem, protection of civil liberties, potential escalation, and the lack of information. These challenges are exacerbated by unclear federal government leadership and confusion during emergencies. Although FERC appears to be the electricity sector lead

---

[314] WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; Barack Obama, President of the U.S., State of the Union Address (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address; Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[315] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012); SECURE IT, S. 2151, 112th Cong. (2012); SECURE IT Act of 2012, H.R. 4263, 112th Cong. (2012); Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (as referred by Senate, May 7, 2012).

[316] S. 2105, §§ 103(b)(1)(c), 110 (giving DHS the lead role in domestic cybersecurity and addressing international cooperation); Donny Shaw, *White House Indicates Support for Cybersecurity Bill that Includes CISPA-Like Language*, OPENCONGRESS, (May 4, 2012), http://www.opencongress.org/articles/view/2490-White-House-Indicates-Support-for-Cybersecurity-Bill-That-Includes-CISPA-Like-Language.

[317] Jennifer Martinez, *Cybersecurity Act Expected to Fail*, THE HILL (Aug. 1, 2012, 7:01 PM), http://thehill.com/blogs/hillicon-valley/technology/241757-cybersecurity-act-expected-to-crash-and-burn-in-senate.

[318] Barack Obama, President of the U.S., State of the Union Address (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address; *see* Presidential Policy Directive 21 (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

and DHS the overall cybersecurity lead, there is still uncertainty in the industry because many organizations appear to do similar research and analysis, and offer similar assistance. There is no clear coordination and leadership. In response to these challenges and this uncertainty, this Article proposes a comprehensive policy to address the unique problems of cybersecurity by offering the following policy recommendations: recognition of responsibility by the government and the industry, information sharing, procurement rules for vendors, federal agency emergency powers, and international cooperation.

After analyzing the existing electricity sector cybersecurity standards and the proposed laws for the electricity sector, it is clear that neither the existing mandatory cybersecurity standards nor the proposed laws address all five components. Both the regulations and the laws need to change to address the shifting leadership roles of the private electric industry and government depending on the timing of the threat and the particular situation. The same regulatory and legal support is necessary for a national-level data aggregator, analysis, and notification center to provide real-time situational awareness of the grid. In contrast, regulatory and legal changes are not necessary for procurement rules if it is a voluntary program, though if procurement rules are mandatory, the NERC standards can be revised to create baseline vendor requirements. NERC could help create a vendor certification program via stakeholder coordination and provide certification program examples from other industries. Laws are better suited for declaring federal agency emergency powers and international cooperation. All three bills dealt with emergency powers, but they failed to even mention the international cooperation needed to address the boundary-less character of cyber threats.

By implementing the five components of cybersecurity detailed in this Article, the electric sector would benefit from improved federal government leadership regarding security threats to our electricity supply. It is also crucial that each critical infrastructure industry works to promote better understanding of the cross sector impacts with workgroups, analysis, scenarios, and exercises.[319] The interconnectedness of cybersecurity and our critical infrastructure cannot be overemphasized.[320] Any future law or policy changes need to be conscious of the critical role of cooperation in any interconnected infrastructure; the electric grid is only the beginning.

[319] *See generally* CRITICAL INFRASTRUCTURE ROADMAP, *supra* note 8.

[320] Keil Speech, *supra* note 148 (stating that the United States is not an island in the context of cybersecurity).