Fordham Urban Law Journal

Volume 41
Number 4 *Until Civil Gideon: Expanding Access to Justice*

Article 1

March 2016

Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforcable Interoperability Standards

Christopher Bosch
Forhdam University School of Law

SECURING THE SMART GRID: PROTECTING NATIONAL SECURITY AND PRIVACY THROUGH MANDATORY, ENFORCEABLE INTEROPERABILITY STANDARDS

Christopher Bosch[*]

---

[*] J.D. Candidate, Fordham University School of Law, 2015; B.S., Boston College, May 2010. I wish to thank Professor Ron Lazebnik for his valuable insight and advice in developing this Note. I would also like to thank Emily Seiderman, Michael Glenn, Frank Restagno, Justin Mahony, and the *Fordham Urban Law Journal* staff for their editorial contributions. Finally, I would like to thank my loved ones for their constant support and guidance.

INTRODUCTION

The United States electrical grid is a marvelous feat of engineering, with the National Academy of Engineering naming "Electrification" the "Greatest Engineering Achievement of the 20th Century."[1] The extent of the United States electrical grid infrastructure is vast, representing over $1 trillion in assets and 360,000 miles of transmission lines connecting over 6000 power plants.[2] Electricity has been integrated into the daily lives of U.S. citizens in innumerable ways.

---

1. GREATEST ENGINEERING ACHIEVEMENTS OF THE 20TH CENTURY, http://www.greatachievements.org (last visited Apr. 15, 2014).

2. INFRASTRUCTURE SEC. & ENERGY RESTORATION, U.S. DEP'T OF ENERGY, LARGE POWER TRANSFORMERS AND THE U.S. ELECTRIC GRID 5 (2012), *available at* http://energy.gov/oe/downloads/large-power-transformers-and-us-electric-grid-report-june-2012.

While the electrical grid is undoubtedly an impressive human innovation worthy of great respect, it is also outdated.[3] Some equipment that makes up the physical infrastructure has already passed its expected life span.[4] Failing grid equipment was the cause of nearly twenty percent of sustained power outages from 2008 to 2011.[5] In light of the Obama Administration's commitment to developing sources and distribution of renewable energy,[6] some have called into question the ability of the aging grid to suit the demands of today's society, identifying the need to improve the efficiency of power delivery and the incorporation of renewable energy technologies as necessary requisites for the electrical grid of tomorrow.[7]

This "grid of tomorrow" will rely upon the near-instantaneous communication of information made possible by the Internet. Wiring the antiquated grid to the Internet, however, will expose existing vulnerabilities and create entirely new ones.[8] Recent attacks on other utilities around the world, as well as institutions traditionally perceived as being secure from cyber attacks such as banks and stock markets, underscore the reality and imminence of these threats.[9] Cyber attackers can remotely engage in wrongdoing from anywhere in the world using Internet connections, and their profiles are diverse,

---

3. In 2003, the Department of Energy described the electrical grid as "aging, inefficient, and congested, and incapable of meeting future energy needs of the Information Economy without operational changes and substantial capital investment over the next several decades." U.S. DEP'T OF ENERGY, "GRID 2030:" A NATIONAL VISION FOR ELECTRICITY'S SECOND 100 YEARS, at iii (2003), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Electric_Vision_Document.pdf.

4. The average power generating station was built in the 1960s and uses even older technology, while the average substation transformer is forty-two years old with a designed maximum life of forty years. LEXINGTON INST., ENSURING THE RESILIENCE OF THE U.S. ELECTRICAL GRID 23 (2013), *available at* http://www.lexingtoninstitute.org/wp-content/uploads/Postal/EnsuringResilienceofUSElectricalGrid.pdf.

5. N. AM. ELEC. RELIABILITY CORP., 2012 STATE OF RELIABILITY 10 (2012), http://www.nerc.com/files/2012_sor.pdf.

6. "The Obama Administration has called for doubling the amount of U.S. electricity produced by renewable sources, such as wind and solar power, during the next three years to reduce greenhouse emissions that cause global warming." Tom Doggett, *U.S. Electric Grid Needs Major Overhaul: Utility*, REUTERS, Jul. 23, 2009, *available at* http://www.reuters.com/article/2009/07/24/us-usa-electricity-grid-idUSTRE56N0HQ20090724.

7. *See id.*

8. *See infra* Part II.C.

9. *See infra* Part II.A.

ranging from lone hackers to ominous, well-funded government institutions.[10]

While the United States has undertaken efforts to address cybersecurity through legislation and executive action, those efforts have been inadequate in establishing standards for how communications between devices and systems in the complex "Smart Grid"[11] will be secured.[12] Current legislation directs federal agencies to establish these "interoperability standards."[13] However, no mandatory standards have been established and it is unclear from relevant statutory language if the applicable agencies have any true enforcement authority.[14] Implementation of interoperability standards by Smart Grid participants is currently performed on a purely voluntary basis.[15]

The Internet connection required to enable the real-time information exchange that the Smart Grid's devices, technologies, and services will rely upon allows for new digital access points to our nation's electrical grid that might be exploited by cyber attackers.[16] The prospect of such infiltration poses a substantial risk to national security. The same Smart Grid features will also allow for the collection of massive amounts of private consumer data that can detail how, when, and where power is consumed in the home. Illicit interception of this data raises significant personal security and privacy concerns. Allowing the standards that would minimize these national security, personal security, and privacy concerns to remain

---

10. *See infra* Part II.B.

11. The "Smart Grid" is a term used to describe the United States electrical grid after the incorporation of the new technologies, devices, and services, *see infra* Part I.B, that are designed to build upon and transform the traditional electric grid, *see infra* Part I.A. It is also used, at times, to encompass the public and private entities that, as a group, enable the functionality of these technologies, devices, and services. These modernization efforts are ongoing. The Smart Grid is in many ways a term of aspiration; its prevalence is a matter of increasing degree.

12. *See generally infra* Parts III, V.A.1.

13. *See infra* Part III.

14. *See generally infra* Parts III, V.A.1.

15. Because no interoperability standards have been promulgated under applicable legislation and the agency with the responsibility of implementing such standards (the Federal Energy Regulatory Commission) interpreted its legislatively-delegated power as not including the ability to promulgate *enforceable* standards, any private organization's implementation of interoperability standards constitutes voluntary action. *Id.*

16. *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, INTRODUCTION TO NISTIR 7628 GUIDELINES FOR SMART GRID CYBER SECURITY 7 (2010), *available at* http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (source document contains an introduction and three distinct volumes).

voluntary and unenforceable leaves the electrical grid and citizens vulnerable to harm. This Note explores these dangers and discusses why granting the appropriate regulatory entities the authority to develop and institute mandatory, enforceable interoperability standards is the most appropriate means to achieving effective Smart Grid cybersecurity.

Part I of this Note describes the key characteristics of the "Traditional Grid"[17] and the Smart Grid, and sets forth the reasoning behind the transition to the Smart Grid and the key concerns the transition raises. Part II discusses the cybersecurity threats to the Smart Grid by reviewing recent cyber attacks that have affected a broad array of industries. It also considers the various types of cyber attackers and how important data and privacy concerns are implicated in the Smart Grid. Part III reviews legislation and executive action that has played a key role in establishing the Smart Grid cybersecurity landscape thus far, as well as the regulatory roles and authorities this legislation has created. After Part III demonstrates that the industry is currently operating in a voluntary environment free from mandatory government regulations as it relates to the implementation of interoperability standards, Part IV discusses an industry-developed standard analogue that is used to illustrate the possible justifications for, and pitfalls of, such a standard, ultimately concluding that a voluntary standard regime is an inappropriate solution for the Smart Grid. Finally, Part V asserts that a system of federal mandatory enforceable standards applicable to all Smart Grid participants is the best path to defending the important national security and privacy interests endangered by the cyber threats discussed in Part II. It argues that the National Institute of Standards and Technology (NIST)[18] is the appropriate federal entity to develop and issue these mandatory standards. Acknowledging that legislation reconfiguring and reassigning responsibilities and authorities in the Smart Grid will be necessary to follow that

---

17. The "Traditional Grid" is the electrical grid as described in Part I.A without the Smart Grid technologies, devices, and services described in Part I.B.

18. NIST is a federal agency within the U.S. Department of Commerce whose "mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." *NIST General Information*, NAT'L INST. STANDARDS TECH., http://www.nist.gov/public_affairs/general_information.cfm (last visited Apr. 13, 2014). NIST has been tasked with developing information system standards relevant to this Note under both the Federal Information Security Management Act of 2002 and the Energy Independence and Security Act of 2007. *See infra* notes 170–88, 295–300.

recommended path, Part V concludes with key elements of a legislative proposal and a depiction of how the resulting regulatory environment might operate to effectuate better Smart Grid cybersecurity.

I. THE EVOLVING ELECTRIC GRID

Before analyzing the benefits and challenges of the substantial transition from the antiquated Traditional Grid to the prospective Smart Grid, it is important to first assess the composition of each, as well as their significant points of difference.

A. The Traditional Grid

The Traditional Grid is a phrase used in this Note to depict the electrical grid as it existed before the recent modernization efforts that characterize the Smart Grid. While it is conceptually helpful to conceive of the Traditional Grid as distinct from the Smart Grid in this manner so that the Smart Grid's contributions and impact can be more clearly identified, it is important to note that much of the Traditional Grid's infrastructure and regulatory environment persists today as the foundation upon which change is being enacted. Therefore, establishing a working understanding of the Traditional Grid's composition and unique regulatory features is critical before expounding the Smart Grid's novel features and the transitional issues to which they give rise.

1. Composition

In the Traditional Grid, the path of electricity is comprised of three main activities: generation, transmission, and distribution.[19]

At "generation stations," electricity is generated through the use of various fuel sources.[20] Sometimes these stations are owned by the same utilities that serve the end customer, while others are owned by Independent Power Producers (IPPs), or the customer itself.[21] While electric utility companies today still enjoy status as permissible "natural monopolies," prior to the enactment of the Public Utilities

---

19. U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS 5–6 (2004), *available at* http://emp.lbl.gov/sites/all/files/interim-rpt-Aug-14-blkout-03.pdf.

20. Such sources include, for example, nuclear, coal, oil, natural gas, hydro power, geothermal, photovoltaic, and others. *Id.*

21. *Id.*

Regulatory Policy Act of 1978 (PURPA), utilities were significantly more vertically integrated.[22]

Once electricity is generated, it must be transmitted across some 360,000 miles of transmission lines.[23] The transmission lines interconnect throughout the nation at various switching stations and substations, forming the power "grid."[24] At a final substation the incoming high-voltage power is "stepped down" to safer levels for distribution to consumers,[25] commonly by way of the familiar overhead poles and wiring or underground systems.

This generation-to-consumer model operates within a continental electrical infrastructure. The continental United States is comprised of three distinct power grids: the "Eastern Interconnection," the "Western Interconnection," and the "Texas Interconnection."[26] The Eastern Interconnection includes the eastern two-thirds of the nation, while the Western Interconnection includes the western third, with the Texas Interconnection serving only most of Texas.[27]

Each of these Interconnections currently operates independently; however, efforts are underway to connect all three at the "Tres Amigas Superstation."[28] Currently, within each interconnection, electricity flows along the paths of least resistance, is used almost the instant it is produced, and "flows over virtually all transmission lines from generators to loads."[29] This means, as the Supreme Court articulated, "any electricity that enters the grid immediately becomes a part of a vast pool of energy that is constantly moving in interstate commerce."[30] Therefore, the Tres Amigas Superstation would create a national pool of energy that can be shared between any and all

---

22. A vertically integrated entity owns operations in multiple levels of the electrical supply chain (including generation, transmission, and distribution). *See* James D. Elliott, *Electric Utility Regulation Reform in New York: Economic Competitiveness at the Expense of the Environment?*, 13 PACE ENVTL. L. REV. 281, 285 (1995). PURPA forced utilities to purchase electric power from IPPs and other "small power production facilities," increasing competition at this level of the grid and reducing the degree of monopolistic dominance by utilities in the electricity industry. *See* 16 U.S.C. § 824a-3(a) (2012); Elliott, *supra*, at 291–92.

23. INFRASTRUCTURE SEC. & ENERGY RESTORATION, *supra* note 2.

24. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 19, at 6.

25. *Id.* at 4.

26. *Id.*

27. *Id.*

28. Kevin Bullis, *Superconductors to Wire a Smarter Grid*, MIT TECH. REV. (Nov. 12, 2009), http://www.technologyreview.com/news/416253/superconductors-to-wire-a-smarter-grid.

29. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 19, at 6.

30. New York v. Fed. Energy Regulatory Comm'n, 535 U.S. 1, 2 (2002).

states in the continental United States. This pool would allow for more reliable and less costly distribution of energy, including renewable energy. For example, the availability of wind energy would grow less dependent on regional weather,[31] and the renewable energy developed in the wind-blown Texas Panhandle would no longer be "trapped" in the Texas Interconnection.[32]

2. Utilities as Natural Monopolies

Massive fixed-cost capital is required to enter the generation, transmission, and distribution markets. Both government and private parties recognized this fact in the Traditional Grid's early days and concluded that it would be wasteful of societal resources to allow for regular competition.[33] Thus, a "compact of sorts" was formed between utilities and the people: utilities would be granted monopolies over certain geographical regions in exchange for subjecting themselves to intensive regulation, including rate-setting, in an arrangement "alien to the free market."[34] Utilities are thus considered permissible "natural monopolies."[35]

Utilities secure designation as natural monopolies from state and local governments, the right to freedom from local competition, a guaranteed market base, delegated eminent domain powers, guaranteed revenues to remain solvent, guaranteed fair rates of return on prudent capital investments, and lower costs of borrowing as a result of this bargain.[36] At the same time, state governments retain substantial regulatory oversight and the ability to set prices (and thus ensure fair and non-discriminatory prices for ratepayers).[37]

This "compact" is relevant to the focus of this Note because as electric utilities evolve from their business model of the last century

---

31. *See* Karen Uhlenhuth, *Tres Amigas Seeks to Break US Grids Out of Isolation*, MIDWEST ENERGY NEWS (Sept. 5, 2013), http://www.greentechmedia.com/articles/read/tres-amigas-seeks-to-break-u.s.-grids-out-of-isolation (providing the example that the wind in Kansas may be producing at different times than the wind in Texas, and the flexibility provided by the Tres Amigas station would make it possible to take advantage of that diversity in the weather).

32. *See id.*

33. Elias L. Quinn & Adam L. Reed, *Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act*, 81 U. COLO. L. REV. 833, 844–45 (2010).

34. Jersey Cent. Power & Light Co. v. Fed. Energy Regulatory Comm'n, 810 F.2d 1168, 1189 (D.C. Cir. 1987).

35. *See* Katharine Southard, *U.S. Electric Utilities: The First Public-Private Partnerships?*, 39 PUB. CONT. L.J. 395, 401 (2010).

36. *See id.* at 402.

37. *See* Elliott, *supra* note 22, at 298; Quinn & Reed, *supra* note 33, at 845–46.

to become more diversified businesses engaging in transactions beyond regional rate schemes, questions regarding the compact's validity may rise to the surface. Challenges to traditional monopoly protections and state jurisdiction may create significant tensions amongst the Smart Grid stakeholders, especially customers who have limited, if any, alternative market options should they grow discontent with their utility's behavior.

B. The Smart Grid

While the Smart Grid is developing upon the existing infrastructure of the Traditional Grid, it has a number of distinguishable features that both provide significant benefits and present significant transitional challenges.

1. Distinguishing Features

NIST identified seven categories of participants—or "domains"—within the Smart Grid, the first three of which have already been mentioned: (1) Bulk Generation, (2) Transmission, (3) Distribution, (4) Customer, (5) Markets, (6) Operations, and (7) Service Provider.[38] While electricity only flows between (1) and (4), all domains exchange digital communications that must be adequately secured.[39] Ultimately, the Smart Grid will likely result in dramatic changes to each domain; however, some of the most distinctive and important changes will be taking place in the Customer, Markets, Operations, and Service Provider domains.

In the Customer domain, two types of Smart Grid technologies are crucial. First, the "Smart Meter" replaces the simpler analog meter on the side of most homes today and uses digital technology to record customer consumption information on a frequent basis (potentially minute-to-minute or greater frequency as technology progresses), with the information regularly transmitted over the Smart Grid

---

38. *See* CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS AND TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 1, SMART GRID CYBER SECURITY STRATEGY, ARCHITECTURE, AND HIGH LEVEL REQUIREMENTS 14 (2010), [hereinafter NIST GUIDELINES VOL. 1], *available at* http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (source document contains an introduction and three distinct volumes).

39. *See id.* at 14, 17 (identifying unique communication paths—or "logical interfaces"—between Smart Grid participants).

network to various entities that can derive value from that information.[40]

"Technologies, devices, and services that access and leverage energy usage information, such as smart appliances that can use energy data to turn on when energy is cheaper or renewable energy is available," represent the second crucial Smart Grid technology in the Customer domain.[41] Smart Appliances are equipped for communication with Smart Meters and allow for the recording of extremely granular, appliance-specific consumption data.[42]

In 2009, Vice President Joe Biden stated in a report to President Obama that eight million homes had been equipped with Smart Meters and declared projections of twenty-six million homes by 2013, and forty million by 2015.[43] But in May 2012, almost one-in-three households had a Smart Meter, with thirty-six million Smart Meters having been installed, and it was projected that sixty-five million Smart Meters would be installed by 2015—more than twenty-five million above Vice President Biden's 2009 estimate.[44] The torrent pace at which this nascent technology is being deployed underscores the importance of establishing mandatory interoperability standards early on to ensure a more secure grid.

In the Markets and Operations domains, it can be expected that businesses will communicate information "across organizational boundaries, thus posing trust issues,"[45] when, for example, a utility

---

40. Andreas S.V. Wokutch, *The Role of Non-Utility Service Providers in Smart Grid Development: Should They Be Regulated, and if So, Who Can Regulate Them?*, 9 J. TELECOMM. & HIGH TECH. L. 531, 534 (2011).

41. NAT'L SCI. & TECH. COUNCIL, EXECUTIVE OFFICE OF THE PRESIDENT, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE 1 (2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

42. CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS AND TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 27 (2010) [hereinafter NIST GUIDELINES VOL. 2], *available at* http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (source document contains an introduction and three distinct volumes).

43. Memorandum from Joseph Biden, Vice President of the United States, to Barack Obama, President of the United States 5 (Dec. 15, 2009), *available at* http://www.whitehouse.gov/sites/default/files/administration-official/vice_president_memo_on_clean_energy_economy.pdf.

44. INST. FOR ELEC. EFFICIENCY, UTILITY-SCALE SMART METER DEPLOYMENTS, PLANS, & PROPOSALS 1 (2012), *available at http://*www.edisonfoundation.net/iee/.../iee_smartmeterrollouts_0512.pdf; INST. FOR ELEC. EFFICIENCY, UTILITY-SCALE SMART METER DEPLOYMENTS: A FOUNDATION FOR EXPANDED GRID BENEFITS 1–2 (2013), *available at* http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterUpdate_0813.pdf; Memorandum, *supra* note 43, at 5.

45. NIST GUIDELINES VOL. 1, *supra* note 38, at 44.

shares collected data with marketers or contractors assisting in the provision of electricity. With the new mass of information that will be accrued through Smart Grid technologies, it can also be expected that "many customers, possibly through aggregators or other energy service providers, will participate in the retail energy market, thus vastly increasing the number of participants."[46] The Markets and Operations domains will have to adapt to the advent of these new entrants in the Service Provider domain.

These "other energy service providers," also referred to as "Edge Service Providers" or "Non-Utility Service Providers" (ESPs) will operate in the Smart Grid not as providers or energy consumers, but as businesses that "utilize the information produced by advanced meters and other utility-deployed smart grid technologies in innovative ways."[47] They might assist consumers in analyzing their electricity consumption to help eliminate inefficiencies and lower electrical bills,[48] or offer a management system that allows consumers to control electric usage in their residence remotely in an innovative, cost-saving manner.[49]

Essentially, there is no question that the Smart Grid will probably result in dramatic changes across a transformed electrical industry. Utilities will perform new functions, ESPs will bypass the utility and derive their own value from customer consumption data, and utilities will sell customer information to marketers. Amongst these likely outcomes, one common theme emerges: massive caches of consumer data will be generated and communicated via the Internet across inter- and intra-organizational boundaries and digital channels in a manner that is alien to the functioning of the Traditional Grid.

---

46. *Id.*

47. Quinn & Reed, *supra* note 33, at 843 n.27.

48. *See* Wokutch, *supra* note 40, at 535–36 (discussing "Electric Efficiency Analysis" solutions, such as Google's PowerMeter, which provides an online web portal for monitoring home energy consumption).

49. One such "Energy Management" solution is AlertMe Energy, which requires attachment of hardware to the consumer's electric meter and a broadband hub that collects and transmits usage data over the Internet to a United Kingdom-based software company's cloud-based application, which can read signals from compatible "smart" appliances, allowing consumers to control the appliances remotely through a web browser or smartphone. *See id.* at 536–37; Heather Clancy, *AlertMe Supports Lowe's Residential Energy Management Platform*, GREENTECH PASTURES (July 24, 2012), http://www.zdnet.com/alertme-supports-lowes-residential-energy-management-platform-7000001494.

2. Benefits

The Smart Grid's benefits are substantial, which Congress recognized by allocating $4.5 billion for electricity delivery and energy reliability modernization efforts through the American Recovery and Reinvestment Act of 2009 (ARRA).[50] The Department of Energy (DOE) issued ninety-nine grants totaling $7.8 billion[51] through its Smart Grid Investment Grant Program to accelerate development of the Smart Grid.[52]

The DOE has identified five primary Smart Grid Technologies that will provide key benefits of resiliency, reliability, environmental stewardship, security, cost effectiveness, and economic stability/development: (1) the Smart Grid Network, (2) Advanced Metering, (3) Phasor Measurement Units, (4) Renewable, Distributed Power Generation, and (5) Energy Storage.

The Smart Grid Network is characterized by two-way communications between energy suppliers and customers.[53] This scheme allows customers to transmit near-real-time consumption information to utilities, while utilities can in turn communicate near-real-time energy pricing back to consumers.[54] Utilities can thus more effectively monitor and manage electrical loads and demands given their access to comprehensive "live" data, while allowing customers to adjust their consumption patterns based on real-time pricing information.[55] Such two-way communication also facilitates more

---

50. *See* NAT'L SCI. & TECH. COUNCIL, *supra* note 41, at 2.

51. $3.4 billion originated from ARRA funding, with an additional $4.4 billion coming from private sector investments. Joseph Paladino, *Energy Department's Investment Grant Program Advances Rapidly, as Scheduled*, IEEE SMART GRID NEWSLETTER (Feb. 2013), http://smartgrid.ieee.org/february-2013/793-energy-department-s-investment-grant-program-advances-rapidly-as-scheduled.

52. *Id.*

53. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, STUDY OF SECURITY ATTRIBUTES OF SMART GRID SYSTEMS—CURRENT CYBER SECURITY ISSUES 4 (2009), *available at* http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf.

54. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0, at 21 (2010) [hereinafter NIST FRAMEWORK RELEASE 1.0], *available at* http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

55. For example, if prices are highest when demand is at its peak, a customer, armed with the knowledge of sky-high energy prices at those peaks, may choose to conserve, allowing for "peak load reduction," a two-way benefit (price savings and reduced strain on the grid). *See* OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 53, at 4. The enabling of these customer choices "based on how, when,

appropriate and proactive utility responses to power outages.[56] "Advanced Metering Infrastructure," including Smart Meters and Smart Appliances, is central to the realization of these network benefits.[57]

Phasor Measurement Units dramatically alter the landscape of the Bulk Generation and Transmission domains. These pieces of equipment allow the grid to sense problems quickly and respond effectively.[58] It was perhaps the capabilities of this equipment that President Obama was alluding to in his 2013 State of the Union Address when he made reference to the notion of "self-healing power grids."[59]

Enhanced responsiveness in the Smart Grid allows for better integration of renewable energy sources such as solar and wind energy sources, which "cannot be turned on or off as needed."[60] A wired grid engaging in two-way communications and equipped with high-tech sensors allows the grid to adjust to these inherent variations in output by drawing energy from other sources when needed.[61]

---

and how much electricity they use" is a touted benefit of the Smart Grid. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 3.

56. *See* OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 53, at 4–5.

57. *See* CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 3, SUPPORTIVE ANALYSES AND REFERENCES app. F-1 (2010) [hereinafter NIST GUIDELINES VOL. 3], *available at* http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf (source document contains an introduction and three distinct volumes). "Advanced Metering Infrastructure" includes the hardware and software that creates a "bi-directional network" between advanced metering equipment (e.g., Smart Meters and Smart Appliances) and a utility's systems, "enabling collection and distribution of information to customers and other parties." *Id.*

58. Phasor Measurement Units will "enhance the situational awareness of the national grid and enable system operators to react to system disturbances and anomalies more accurately and expeditiously." OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 53, at 6. These high-tech devices will be placed throughout the grid and take precise measurements of voltages, currents, and frequency, communicating that information back to grid operators at high speed. *See id.* Combining the data from all Phasors throughout the grid will provide operators with a comprehensive picture of the nation's grids in any given area, and by developing "advanced operating procedures/algorithms," the data can be used to allow for automated responses by the grid to stimuli, potentially avoiding or mitigating power outages, quality problems, and service disruptions. *See id.*

59. President Barack Obama, 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.

60. NAT'L SCI. & TECH. COUNCIL, *supra* note 41, at 14. For additional information regarding how Smart Grid technologies will foster the integration of renewable energy sources, see generally *id.* at 13–14, 25.

61. *See* OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 53, at 6.

Finally, advances in energy storage technologies mean that, in the Smart Grid, energy can be stored for later consumption when it is least expensive to generate, allowing for reduced peak loads. This reduces strain on the system and increases cost savings.[62] Such energy storage could also serve significant benefits in times of crisis, such as the August 2003 Northeast blackout[63] or 2012's Hurricane Sandy.

While these substantial benefits offer great promise for consumers, businesses, and the United States' energy future, their realization calls for fundamental changes to the Traditional Grid that present a number of challenges.

C. Transition Issues

The Smart Grid carries with it many fundamental changes for a variety of stakeholders. For the utility industry, it means a transition from a business model of purely supplying electricity to a hybrid business model where energy delivery is coupled with other services revolving around the collection and management of granular customer consumption data.[64] Customers will be presented with new opportunities to monitor and adjust their electricity consumption. For ESPs, the Smart Grid presents new business prospects. While promising in some regards, such unfamiliar activity occurring on such a large scale in an industry that is inextricably intertwined with virtually every aspect of everyday life represents a formidable undertaking.

Utilities face the challenge of first making *possible* the sophisticated power-flow management noted above,[65] and then *providing* that kind of meticulous distribution effectively.[66] While the idea of utilizing live data from Phasor Measurement Units and Smart Meters to adjust transmission, distribution, and storage of electricity sounds ideal, it represents a stark contrast from the more straightforward traditional responsibility of providing energy to meet demand. The two-way network outlined above necessarily entails communication between computers, devices, software, and other

62. *See id.* at 7.
63. *See id.*
64. *See* Quinn & Reed, *supra* note 33, at 842.
65. *See supra* notes 53–64 and accompanying text.
66. *See* NIST GUIDELINES VOL. 1, *supra* note 38, app. B-1.

technologies that present national security threats posed by hackers and other cyber attackers that did not exist in the Traditional Grid.[67]

While the customer data noted above will allow for worthwhile benefits, the Smart Grid will "greatly expand the amount of data that can be monitored, collected, aggregated, and analyzed," which will raise significant privacy concerns.[68] Time-stamped dwelling activity reports being transmitted over the Internet, if intercepted, could reveal personal and intimate details that may give rise to personal security concerns, such as a computer-savvy thief detecting when a dwelling has gone empty for an extended period of time.[69]

The Smart Grid will allow for enhancements in efficiency and reliability through the collection of massive amounts of granular data collected from Smart Meters and various points in the transmission system. However, if this new Internet-enabled Smart Grid is not properly secured, access to its systems by wrongdoers could lead to devastating consequences.

II. THE CYBERSECURITY THREAT

The Smart Grid will rely on Internet connectivity in moving massive amounts of data through many channels and entities in order to fully capture the data's potential value.[70] With such extensive digital communication occurring, the possibility of illicit interception or manipulation of those communications increases.[71] In the Smart Grid realm, cyber intruders, in many ways, have the upper hand. To this point, they have been successful in breaching some of the most secure operations in the world, including electrical utilities, nuclear programs, an oil company, banks, and a stock exchange.[72] While the popular view of a hacker may be a single computer-savvy individual, institutional hacking is also prevalent today.[73] More sophisticated

---

67. *See* NAT'L SCI. & TECH. COUNCIL, *supra* note 41, at 49 (noting that "a smarter grid includes more devices and connections that may become avenues for intrusions, error-caused disruptions, malicious attacks, destruction, and other threats").

68. NIST GUIDELINES VOL. 3, *supra* note 57, at 19.

69. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 11.

70. *See id.* at 29–33 (identifying the types of data that can be collected in the Smart Grid and the different ways in which that data is valuable to interested parties).

71. *See* NIST GUIDELINES VOL. 1, *supra* note 38, at 6 (explaining that as the grid becomes "smarter" it will contain "more interconnections that may become portals for intrusions, error-caused disruptions, malicious attacks, and other threats").

72. *See infra* Part II.A.

73. *See, e.g.*, Michael Kelley & Geoffrey Ingersoll, *How the US Invited Iranian Hackers to Attack America's Banks*, BUS. INSIDER (Oct. 18, 2012), http://www.businessinsider.com/us-started-worldwide-cyberwar-hacking-2012-

attacks can be launched with the added resources behind such operations.[74]

One issue in responding to these threats is that securing the grid is expensive. In 2010, Pike Research, a "Cleantech Market Intelligence Firm," estimated that in the following five years there would be a cumulative investment in Smart Grid security of $21 billion, representing approximately fifteen percent of all Smart Grid capital investments.[75] While these numbers may seem large, some wonder if enough is being spent. Pike Research stated in a 2011 report that "[u]tility cyber security is in a state of near chaos. After years of vendors selling point solutions, utilities investing in compliance minimums rather than full security, and attackers having nearly free rein, the attackers clearly have the upper hand."[76] The report cited the lack of enforceable standards as a reason for the chaos and a hindrance to action since it causes utilities and vendors to take a "wait-and-see posture" until the regulatory environment becomes clearer, rather than act now and risk "losing their entire investment if future laws invalidate their approach."[77]

Conversely, cyber attacks can be relatively inexpensive to execute. This is because the "defense needs to be strong everywhere, while the offense only needs to succeed in one place;" once a hacker gains access to a network, the whole network may be compromised if the breach goes undetected or insufficient procedures are in place to quarantine the breach.[78] This concern is important to the Smart Grid, where the communication network will become increasingly complex in both the Operations and Service Provider domains, increasing the

---

10#ixzz2HhqDtUMP (reporting that more than one hundred-forty countries are actively developing cyber-espionage and warfare capabilities).

74. *See, e.g.*, Lee Ferran, *Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet*, ABC NEWS (July 9, 2013), http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet (stating that some cyber weapons are so sophisticated and expensive that cybersecurity experts believe they can only be attributable to nations).

75. *See Smart Grid Cyber Security Market to Reach $3.7 Billion by 2015, According to Pike Research*, BUS. WIRE (June 23, 2010), http://www.businesswire.com/news/home/20100623005613/en/Smart-Grid-Cyber-Security-Market-Reach-3.7.

76. PIKE RESEARCH, UTILITY CYBER SECURITY: SEVEN KEY SMART GRID SECURITY TRENDS TO WATCH IN 2012 AND BEYOND 1 (2011), *available at* http://www.navigantresearch.com/wp-assets/uploads/2011/11/UCS-11-Pike-Research.pdf.

77. *See id.* at 5.

78. Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 455 (2012).

system's vulnerability with added access points.[79] Additionally, operators and consumers will seek to control equipment (valves and switches for utilities, appliances for consumers) remotely through the Internet—types of remote connections that could "allow[] attackers a gateway into the system."[80] The damage that can be caused by this type of breach was demonstrated in 2007, when the Department of Homeland Security performed the staged "Aurora" experimental remote attack on a generator that was part of a replicated power plant's control system.[81] Researchers were able to "change[] the operating cycle of the generator, sending it out of control."[82] In a released video, the generator jerks violently several times before the equipment begins to fail, ultimately releasing massive amounts of white and black smoke upon its destruction.[83] The Aurora experiment would come to foreshadow malicious cyber attacks on various institutions all over the world.

A. Recent Attacks

The staged Aurora attack perhaps marked the first moment of widespread public awareness that digital communication in critical infrastructure operations was a double-edged sword. On the one hand, it offers cost savings, convenience, and efficiency, but on the other hand, it creates dangerous vulnerabilities. Although the implications of Aurora were frightening, there was skepticism that such an attack could or would happen outside a staged environment.[84] That perception would quickly change with the onset of cyber attacks on various energy companies.

---

79. *See* NAT'L SCI. & TECH. COUNCIL, *supra* note 41, at 49 (suggesting that a smarter grid's "[n]etworks of computers, intelligent electronic devices, software, and communication technologies present greater infrastructure protection challenges than those of the traditional infrastructure" as they "may become avenues for intrusions, error-caused disruptions, malicious attacks, destruction, and other threats").

80. Ellen Nakashima & Steven Mufson, *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*, WASH. POST, Jan. 19, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html.

81. The "Aurora" experiment was conducted in March of 2007 at the Department of Energy's Idaho lab. *See* Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk.

82. *See id.*

83. *See id.*

84. *See* Meserve, *supra* note 81 ("Despite all the warnings and worry, there has not been any publicly known successful cyber-attack against a power plant's control system. And electric utilities have paid more attention to electronic risks than many other industries, adopting voluntary cyber-standards.").

In 2008, computer hackers targeting countries other than the United States "literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power."[85] Later that year, a power company hired a "penetration-testing consultant" to test the company's cyber security. The test had to be shut down within hours because the hacking operation was "working too well," with experts citing the power company's system's Internet connectivity as the key vulnerability.[86]

In 2010, the "Stuxnet" computer virus damaged Iran's nuclear program by infiltrating its Supervisory Control and Data Acquisition system (SCADA).[87] At one point, the virus temporarily disabled approximately one-fifth of the plant's centrifuges, which were spinning to purify uranium.[88] While the *New York Times* reported that the United States and Israel developed the virus,[89] neither country's government has officially acknowledged such involvement.[90]

In 2011, the "Night Dragon" cyber attacks targeted global oil, energy, and petrochemical companies, and were believed to have originated in the Shandong Province of China.[91] Also discovered in 2011 was the "Duqu" virus, thought to be an offshoot of Stuxnet, that was aimed more at information gathering than destruction of

---

85. Ted Bridis, *CIA: Hackers Demanding Cash Disrupted Power*, NBC NEWS (Jan. 18, 2008), http://www.nbcnews.com/id/22734229/#.Ulwg5bQvYb6.

86. A hired consultant explained that the heart of utility operations known as SCADA used to be designed as a closed system; however, intranets and the Internet have now been integrated into SCADA, making it vulnerable to cyber attacks. The consultant and his team sent an e-mail to firm employees about a plan to cut their benefits and included a link to "find out more." When that link was clicked, the employee's computer downloaded malware that enabled the consultants to take control of the machine, providing them "full system control." Tim Greene, *Experts Hack Power Grid in No Time*, NETWORKWORLD.COM (Apr. 9, 2008), http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html.

87. STAFF OF CONGRESSMEN EDWARD J. MARKEY & HENRY A. WAXMAN, ELECTRIC GRID VULNERABILITY: INDUSTRY RESPONSES REVEAL SECURITY GAPS 23 (2013) [hereinafter MARKEY REPORT], *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf. For more on SCADA and its importance to power plant operations, see *supra* note 86 and accompanying text.

88. *See* David E. Sanger, *Obama Ordered Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

89. *See id.*

90. *See* Ferran, *supra* note 74.

91. N. AM. ELEC. RELIABILITY CORP., INDUSTRY ADVISORY: "NIGHT DRAGON" (2011), http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-02-18-01%20Night%20Dragon%20FINAL.pdf.

industrial control systems.[92] In 2012, the "Shamoon" virus infected the Saudi Arabian State Oil Company, known as "Aramco," destroying more than 30,000 computers using a code known as a "wiper" that essentially erased all of the data on the computer's hard drives, rendering them useless and irreparable.[93]

At the time of Aurora, electric utilities gave the impression that efforts were at least being considered to enhance cybersecurity through the adoption of "voluntary" cyber standards.[94] One economist suggested that of all the industries, perhaps only banking, finance, and telecommunications had better cybersecurity than the electric industry.[95] Attacks on these perceived security stalwarts in the following years would reinforce the seriousness of the threat of cyber attacks.

One such stalwart, Citibank, was hacked in 2008. Three hackers pled guilty to hacking Citibank ATM card numbers and Personal Identification Numbers to steal $2 million from customer accounts over a period of four months.[96] In 2011, hackers gained access to the data of hundreds of thousands of Citigroup's credit card customers in North America, with one member of the hacker group "Anonymous"[97] describing Citigroup's 128-bit encryption used to protect electronic customer information as "really not that big a deal . . . . The security is so weak right now, if you know a couple attacks, you can just go around and see what works."[98] In October of 2012, then-Secretary of Defense Leon Panetta remarked that the "scale and speed" with which large U.S. financial institutions were

---

92. *See* MARKEY REPORT, *supra* note 87, at 24.

93. *See id.* at 5; Ellen Nakashima, *U.S. Warns Industry of Heightened Risk of Cyberattack*, WASH. POST, May 9, 2013, http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran.

94. *See* Meserve, *supra* note 81.

95. *See id.* (quoting Economist Scott Borg who, at the time, produced security-related data for the federal government of the United States).

96. Kevin Poulsen, *Three Plead Guilty in $2 Million Citibank ATM Caper*, WIRED (Nov. 5, 2008), http://www.wired.com/threatlevel/2008/11/three-plead-gui.

97. "Anonymous" is an "informal hacker collective that often targets groups or countries it sees as enemies of Internet freedom." Max Fisher, *Hacker Group Anonymous Is No Match for North Korea*, WASH. POST, June 27, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea.

98. Chris V. Nicholson & Eric Dash, *Citi Says Credit Card Customers' Data Was Hacked*, DEALBOOK (June 9, 2011, 12:49 PM), http://dealbook.nytimes.com/2011/06/09/citigroup-card-customers-data-hacked/?_r=0.

being hacked was "unprecedented."[99] Attacks in 2012 caused major disruptions to the "online banking sites of Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNS, Capital One, Fifth Third Bank, BB&T and HSBC."[100]

In 2013, Citibank was hacked again, along with PNC Bank.[101] The U.S. Attorney's Office for the Southern District of New York indicated that the hack was allegedly achieved through the use of malware and other targeted cyber attacks, allowing the attackers to steal "hundreds of thousands of bank account numbers, PIN numbers, and other codes to withdraw millions of dollars from victim accounts."[102] The same defendants allegedly hacked NASDAQ by installing malware on NASDAQ servers, allowing them to access the infected servers and "execute commands on those servers, including commands to delete, change, or steal data."[103]

Security breaches over the last six years on energy facilities, financial institutions, and other organizations have demonstrated that individuals and entities possess the knowledge and means to launch successful cyber attacks. The attackers' identities and motives are diverse and should be considered in assessing the nature of the threat to Smart Grid security.

B. Profile of the Attackers

Different parties carry out cyber attacks for different reasons. In 2012, Verizon published a "Data Breach Investigations Report" (the Verizon Report), which provided several useful frameworks for understanding the various types of cyber attackers, their methods of choice, and their underlying motivations.[104]

---

99. Leon E. Panetta, Secretary of Defense, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

100. Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 8, 2013, at B1.

101. Press Release, U.S. Attorney's Office for the S. Dist. of N.Y., Manhattan U.S. Attorney and FBI Assistant Director-in-Charge Announce Charges Against Russian National for Hacking Nasdaq Servers (July 25, 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/July13/KalininandNasenkovIndictmentsPR.php.

102. *Id.*

103. *Id.*

104. VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT (2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (follow "download" hyperlink).

In analyzing 855 breach incident cases,[105] the Verizon Report found that 98% of breaches were performed by external agents, 4% by internal agents, and less than 1% by partner agents.[106] The most commonly employed methods of attack included malware (69% of breaches) and hacking (81% of breaches).[107] In assessing the underlying motivations for attacks, the Verizon Report concluded that 96% of breaches—when considering the entire pool of organizations affected—were motivated at least in part by "Financial or Personal Gain," while "Disagreement or Protest," "Fun, Curiosity, or Pride," and "Grudge or Personal Offense" were cited as motivations in less than 4% of each cases.[108] When narrowing the scope of review to cases involving large organizations, "Financial or Personal Gain" was still a factor in many attacks (71%), however, "Disagreement or Protest" and "Fun, Curiosity, or Pride" played a much larger role in attacking these entities (a motivating factor in 25% and 23% of cases, respectively).[109]

The Verizon Report demonstrates that financial or personal gain is very often a motivating factor in breaches, which is concerning within the context of the Smart Grid, where a primary goal is the generation of large caches of valuable—and what many would consider private—data. Disagreement, protest, or curiosity are likely motivating factors behind some of the troubling state-sponsored hacking groups, such as the Chinese organization known as the "Comment Crew," which is believed to be run either by Chinese army officers or government contractors.[110] Recently, concerns have risen that the goals of the Comment Crew are shifting from stealing data to manipulation of American critical infrastructure, including the power grid.[111]

---

105. These 855 incidents resulted in a collective 174 million compromised records. The breach incident data was accumulated by Verizon with contributions from a number of organizations, including the United States Secret Service, Dutch National High Tech Crime Unit, Australian Federal Police, Irish Reporting & Information Security Service, and London Metropolitan Police. *Id.* at 2.

106. *See id.* at 3. External threat agents are sources outside of the breached organization and its network of partners. *See id.* at 16. These include both entities (e.g., former employees or criminal groups) and environmental events (e.g., floods or earthquakes). Internal threat agents are sources within the breached organization, such as executives or employees. *See id.* Partners are third parties sharing a business relationship with the breached organization (e.g., vendors or outsourced information technology support). *Id.*

107. *See id.* at 3.

108. *See id.* at 19.

109. *See id.*

110. David E. Sanger et al., *China's Army Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, at A1.

111. *See id.*; MARKEY REPORT, *supra* note 87, at 27.

In June of 2012, it is believed the Comment Crew was behind a failed "spearphishing"[112] attack on Digital Bond, a firm that specializes in control system security consulting. The attack sought to trick the recipient into installing a remote-access tool that would have given attackers control over the recipient's computer and, ultimately, access to confidential information about the company's casework, which included security consultation information for a power plant and a major water project.[113]

Perhaps the most disturbing Comment Crew attack occurred in September of 2012, when Telvent, a company that designs software giving oil, gas, and electric grid operators remote access to valves, switches, and security systems, was successfully infiltrated.[114] The attackers used malware and were able to take project files.[115] Telvent cut off access before the attackers could take control of any systems.[116] An employee of Digital Bond said that such an attack is "terrifying" since access to a vendor such as Telvent is the "holy grail" when it comes to acquiring the capability to take out critical systems.[117]

President Obama addressed these events with a call to action during his 2013 State of the Union Address: "Now our enemies are . . . seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing . . . ."[118]

---

112. "Spearphising" is an attack that targets individuals or groups with messages that are designed to seem to originate from a trusted source in an attempt to trick users into performing an act, such as clicking a link or opening an attachment, that would contain a malicious code that allows the attacker to obtain confidential information or unauthorized access to the user's network. *See* N. AM. ELEC. RELIABILITY CORP., *supra* note 91.

113. *See* Sanger et al., *supra* note 110. For more information on the Digital Bond attack and a screenshot of the illegitimate message, see Reid Wightman, *Spear Phishing Attempt*, DIGITAL BOND (June 7, 2012), https://www.digitalbond.com/blog/2012/06/07/spear-phishing-attempt.

114. *See* Sanger et al., *supra* note 110. Telvent was in possession of "detailed blueprints on more than half of all the oil and gas pipelines in North and South America, and ha[d] access to their systems." *See id.*

115. *See* Brian Krebs, *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*, KREBSONSECURITY (Sept. 25, 2012), http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent. It was reported that the attack spanned Telvent operations in the United States, Canada, and Spain. *Id.* The stolen project files "related to one of [Telvent's] core offerings—OASyS SCADA—a product that helps energy firms mesh older information technology assets with more advanced 'smart grid' technologies." *Id.*

116. *See* Sanger et al., *supra* note 110.

117. *See id.*

118. President Barack Obama, *supra* note 59.

C. Data, Privacy, and the Impact on Cybersecurity

The novel operational characteristics of the Smart Grid—particularly utilities' capacity to maintain detailed records of customers' electric energy consumption—give rise to significant privacy concerns that are difficult, if not impossible, for concerned customers to avoid.

1. Smart Grid Privacy Concerns

Barriers in the Traditional Grid that greatly diminished the value of energy consumption pattern data—and thus public concern with its collection—will not exist in the Smart Grid.[119] Utilities will no longer need to send a person or crew to read home meters; data will be transmitted electronically over the Internet.[120] Previously, not much value could be derived from monthly (or more infrequent) meter readings; in the Smart Grid, readings will now be taken multiple times daily.[121] Further, those readings will be far different from the lump-sum energy readings in the Traditional Grid; usage data could be available on a granular appliance-by-appliance level.[122]

While such changes can be characterized as beneficial access that will allow utilities to more efficiently deliver energy and services, they are also more intrusive on personal privacy. We live in an information-sharing age in which choices to share information are often deliberate and voluntary; however, in the Smart Grid, it is not so apparent that this same sense of "choice" will exist.[123] In resisting such sharing, the option of living without an essential utility such as electricity may not be a feasible option at all.[124]

NIST, in carrying out its responsibilities under the Energy Independence and Security Act of 2007 (EISA),[125] developed a Privacy Subgroup to focus primarily on privacy within personal dwellings and electric vehicles.[126] One conclusion that the Privacy

---

119. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 9.

120. *See id.* at 2.

121. *See id.*

122. *See id.*

123. *See generally* Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 216–17 (2011).

124. *See* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 174–75 (2011).

125. Pursuant to 42 U.S.C. § 17385, it is the "primary responsibility" of the Director the NIST to "coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." 42 U.S.C. § 17385 (2012).

126. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 2.

Subgroup reached was that "[m]ost consumers probably do not understand their privacy exposures or their options for mitigating those exposures within the Smart Grid."[127] The Smart Grid reaches into the intimate goings-on of homes and businesses in ways that the Traditional Grid never had.[128] As Cheryl Dancey Balough articulates the issue, "The ability to get rich data from the smart meters, however, might also just be the smart grid's Achilles' heel [from a privacy viewpoint]."[129]

With such detailed energy consumption information being transmitted over the Internet, there is the threat that it can be intercepted by a criminal looking to spy on others to, for example, determine when a family has gone to sleep or embarked on a vacation, or to blackmail top officials.[130] Free market supporters may suggest that it is the consumer's responsibility to educate him or herself on the privacy implications and, once so educated, make an informed decision as to whether or not he or she wishes to participate in the Smart Grid by utilizing its technologies. Faced with threats to privacy posed by Smart Grid technologies like Smart Meters and Smart Appliances, do consumers really have a meaningful choice in deciding whether to use these technologies and expose themselves to such privacy threats?

2. The "Illusion of Choice" in Smart Meter Installation

Smart Meters, especially operating in conjunction with Smart Appliances that wirelessly communicate how much energy they are consuming and when,[131] can "reveal much more detailed information about the activities within a dwelling or other premises than was available in the past."[132] Privy to this reality, customers across the

---

127. *Id.*

128. *See* NIST GUIDELINES VOL. 1, *supra* note 38, at 75 ("As the Smart Grid reaches into homes and businesses, and as customers increasingly participate in managing their energy, confidentiality and privacy of their information has increasingly become a concern. Unlike power system reliability, customer privacy is a new issue.").

129. *See* Balough, *supra* note 124, at 163–64.

130. In 2005, it was reported that "someone with inside access" to the cellphone company, Vodafone, had "been bugging more than 100 high-ranking government officials and dignitaries including the prime minister of Greece, his wife, and the Mayor of Athens." John Markoff, *Engineers as Counterspies: How the Greek Cellphone System Was Bugged*, N.Y. TIMES, July 10, 2007, http://bits.blogs.nytimes.com/2007/07/10/engineers-as-counterspys-how-the-greek-cellphone-system-was-bugged.

131. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 27.

132. *See id.* at 13.

nation have taken issue with their inability to "opt out" of Smart Meter installations at their home, preferring instead to maintain their current mechanical meter and the status quo if possible.[133]

Some Public Utilities Commissions (PUCs), such as Maine's, have ordered utilities to make opting out an option for customers, but have allowed utilities to charge customers a fee to exercise this option—a policy that has also met resistance.[134] The Supreme Judicial Court of Maine recently held in *Friedman v. Public Utilities Commission* that utilities retain discretion as to what equipment is used in conjunction with their provision of services.[135] The court held that the customers permitted the utility to choose what meter it would use "by virtue of their agreement to purchase service from [the utility]."[136] Thus, utilities could swap out a mechanical meter for a Smart Meter at their discretion unless the customer elected to opt out of the installation, in which case an opt-out fee would be imposed. One problem with the contractual argument the court set forth in this case is that since utilities operate in a monopolistic environment free from local competitors,[137] a utility contract can take on an adhesive "take-it-or-leave-it" character, leaving residents with no option to choose another electric energy provider and questionable legal recourse despite their legitimate privacy concerns.

---

133. *See Where Smart Meters are Optional/Free or Free*, CENTER FOR ELECTROSMOG PREVENTION, http://www.electrosmogprevention.org/stop-ca-smart-meter-news/where-smart-meters-are-optional (last visited Apr. 13, 2014) (providing resources and discussions of opt-out policies and legislation in various states).

134. The penalized customers have argued that incentives for "opting in," as opposed to penalties for "opting out," given the nature of their health and privacy concerns, would be more appropriate. *See* Ten-Person Complaint Pursuant to 35-A M.R.S.A. Section 1302 Regarding "Smart Meters" & "Smart Meter" Opt-Out as Promulgated by the Maine Public Utilities Commission (MPUC), No. 2011-00262 (Me. Pub. Utils. Comm'n Aug. 1, 2011). In California, PG&E has instituted a similar opt-out fee policy, claiming that the fees are to cover installing analog meters in homes that already had Smart Meters installed but want to switch back, as well as worker wages for monthly meter readings since it would not be "fair to expect neighbors who keep their SmartMeters to have to pay for the cost of the meter reader." Dana Hull, *PG&E Customers Can Opt Out of SmartMeters—For $75, Plus $10 a Month*, SAN JOSE MERCURY NEWS, Feb. 1, 2012, http://www.mercurynews.com/breaking-news/ci_19869073.

135. Friedman v. Pub. Utils. Comm'n, 48 A.3d 794 (Me. 2012).

136. *Id.* at 801. The Terms and Conditions gave the utility the right to select and alter the metering equipment used in conveying electricity to the customer, as well as the right to access the customer's property to inspect, repair, or remove the utility's property. *Id.*

137. Utilities are considered natural monopolies and are permitted to operate free from local competition as a result of a compact with state governments that will carry over from the Traditional Grid. *See supra* Part I.A.

Even if Smart Meters are financially imposed upon consumers in this manner, some may argue that consumers still have a free market choice that will allow them to avoid this privacy exposure: they can refuse to purchase the Smart Appliances that communicate appliance-specific data to Smart Meters. Unfortunately, this solution is not very effective given the inferences that can be drawn from the granular data accumulated by Smart Meters.

Customer electrical consumption activities can be inferred due to one crucial difference between the utility's mechanical meter in the Traditional Grid and the Smart Meter: the frequency with which meter readings are taken. In the Traditional Grid, a utility employee might have recorded readings monthly.[138] Meanwhile, Smart Meters are designed to allow for readings in fifteen-minute intervals, if not less.[139] Even if the Smart Meters did not communicate with Smart Appliances and only recorded lump sum electrical consumption, the frequency with which the data is recorded allows for inferences as to what types of appliances are being used based on what is known about the manner in which different appliances consume electricity.[140] If Smart Appliances that communicate directly with Smart Meters become more popular in households, they would only remove the need for such inference. The revealing data would then be conveyed over the Internet to utilities and possibly other Smart Grid participants like ESPs, insurance companies, or marketers.[141] Strong cybersecurity is necessary to prevent illicit interception of that data.

Government efforts to gain access to these detailed records for investigatory purposes have also raised significant issues. In addition

---

138. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 13–14.

139. *Id.*

140. Appliances produce "signatures" that allow someone analyzing an otherwise anonymous set of data to identify when certain appliances are being used. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 16, at 19. The signatures are created by the unique manner in which certain appliances consume energy. Research has indicated that a review of electricity consumption data for appliance signatures can reveal when, throughout the day, a refrigerator comes on, a kettle is activated, a toaster is used, clothes are washed, and an oven is preheating. *See* ELIAS L. QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES 3 (2009), *available at* http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf. NIST documentation suggests that "[a]s the time intervals between smart meter data collection points decreases, appliance use will be inferable from overall utility usage data and other Smart Grid data with even greater accuracy." *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 14.

141. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 29–33.

to Fourth Amendment concerns,[142] NIST, journalists, and scholars have demonstrated how efforts by the government to legally require that Internet communication providers build "backdoors" into their communication systems to enable government wiretapping, if successful, would increase the vulnerability of Internet communication networks like the Smart Grid.[143] These government

---

142. For thorough and insightful discussions of the Smart Grid's Fourth Amendment implications, see generally Balough, *supra* note 124; McNeil, *supra* note 123.

143. NIST documentation has noted that "[c]urrent law both protects private electronic communications and permits government access to real-time and stored communications, as well as communications transactional records," citing the Electronic Communications Privacy Act as an example. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 12. Those documents also cited a law important to the Smart Grid Fourth Amendment discussion known as the Communications Assistance for Law Enforcement Act (CALEA), which requires "telecommunications carriers and equipment manufacturers . . . to design their systems to enable lawful access to communications." *Id.* In addition to the Fourth Amendment concerns related to government surveillance of in-home activities such a law raises, the law could also lead to system vulnerabilities. By building in "back doors" for government wiretapping, access points are created where none existed before, and wrongdoers who successfully gain access to them can exploit them in malicious ways. A New York Times article cited an instance in Greece where it was "discovered that hackers had taken advantage of a legally mandated wiretap function to spy on top officials' phones, including the prime minister's." Charles Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&. For more on the Greek scandal, see generally Markoff, *supra* note 130; Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair: How Some Extremely Smart Hackers Pulled Off the Most Audacious Cell-Network Break-In Ever*, IEEE SPECTRUM (June 29, 2007), http://spectrum.ieee.org/telecom/security/the-athens-affair.

It has been noted that while some communications service providers are beyond CALEA's reach, federal law enforcement officials have been seeking new legislation that would require Internet communication providers to similarly establish "back doors" so that companies like BlackBerry, Facebook, Skype, and e-mail providers would be technically capable of complying with a wiretap order. *See* Savage, *supra*. The two-way communication central to Smart Grid functionality could foreseeably qualify utilities as Internet communication providers under the desired law. The result "would include being able to intercept and unscramble encrypted messages . . . . Several privacy and technology advocates argued that requiring interception capabilities would create holes that would inevitably be exploited by hackers." *Id.*

More recent reports have indicated that the FBI is growing impatient with legislative delays in creating CALEA-like requirements for Internet communication providers and is "quietly pushing its plan to force surveillance backdoors on social networks, VoIP, and Web e-mail providers . . . asking Internet companies not to oppose a law making those backdoors mandatory." Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET (May 4, 2012), http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/?part=rss&subj=news&tag=title.

efforts to wiretap digital communications create additional privacy and security concerns that consumers may wish to avoid by choosing not to utilize Smart Meters or Smart Appliances, only to discover that they lack the ability to freely exercise such choices.

Should states follow Maine's approach of relying upon contract language in granting utility companies the discretion to choose metering equipment, the monopolistic nature of the Traditional Grid would leave consumers without a meaningful choice in using Smart Meters, unless they choose to bear a penalty for opting out. Even in a state where there is no charge for opting out[144] or an "opt in" program is established, an increase in popularity of the Smart Grid and the prevalence of its technologies may make older technologies obsolete, indirectly pushing hesitant consumers into the Smart Grid over time.[145] Refusing to purchase Smart Appliances does not solve the problem because the increased frequency of consumption recordings allows for inferences of appliance usage. Whether consumers participate in the Smart Grid by choice or by compulsion, there should be a uniform, mandated approach to securing their consumption data given the intimate, private details it can reveal; details of the sort that should not be compromised by advancements in technology.[146]

III. EFFORTS TO ADDRESS CYBERSECURITY: THE CURRENT LEGISLATIVE AND REGULATORY ENVIRONMENT

Congress and the Obama Administration have demonstrated an awareness of the dangers that cybersecurity vulnerabilities pose to national security and, in response, have factored these concerns into

---

For additional information regarding "backdoors" and the vulnerabilities they can create in otherwise secured systems, see Swire & Ahmad, *supra* note 78.

144. Utilities in Vermont have been prohibited from charging customers Smart Meter opt-out fees. *See Vermont Legislature Eliminates Smart Meter Opt-Out Fee*, WAKE UP, OPT OUT! (May 8, 2012), http://wakeupoptout.org/2012/05/vermont-legislature-eliminates-smart-meter-opt-out-fee.

145. As one scholar notes, even if a customer could legally opt out of the Smart Meter program, "his or her choice can in practice only be honored so long as their chosen alternative remains both available and technologically compatible with the electric grid, which is itself also in transition." McNeil, *supra* note 123, at 201 n.20.

146. The Supreme Court has acknowledged the threat to privacy posed by advancements in technology. In *Kyllo v. United States*, the Supreme Court held that the obtaining of information by sense-enhancing thermal imaging technology that could not otherwise be obtained except by physical intrusion constituted an unlawful search, and noted that "[i]n the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes." 533 U.S. 27, 37 (2001) (emphasis in original).

legislation, executive orders, and project funding requirements. However, these responses have been inadequate in the Smart Grid context. In an industry as fast-moving as the Smart Grid, mandatory interoperability standards must be established early if they are going to be established at all. Instead, a voluntary adoption regime persists to the potential detriment of citizens and businesses.[147]

While a self-regulatory model[148] can be effective in regulating an industry, the model established through the Energy Policy Act of 2005 (EPAct)[149] (which amended the Federal Power Act (FPA)) to develop mandatory reliability standards does not fully address Smart Grid cybersecurity from the interoperability perspective. The separate regulatory relationship established between NIST and the Federal Energy Regulatory Commission (FERC) under the EISA to implement interoperability standards is too burdensome and inactive to appropriately account for the fast-moving nature of Smart Grid development.[150] While all interoperability standards remain voluntary, utilities will continue to pick and choose what standards to abide by, often opting for minimum security to save money. Profit generators, such as Smart Grid technologies, will likely continue to be produced amongst a patchwork of inconsistent state and/or industry interoperability standards, rendering the Smart Grid highly vulnerable to cyber attacks.[151]

---

147. As noted by the NIST, "Without standards, there is the potential for these . . . investments to become obsolete prematurely or to be implemented without measures necessary to ensure security." NIST FRAMEWORK RELEASE 1.0, *supra* note 54, at 7.

148. A self-regulatory model is one in which the industry to be regulated develops the standards that will eventually regulate it. *See* DAVID DOLEZILEK & LAURA HUSSEY, REQUIREMENTS OR RECOMMENDATIONS? SORTING OUT NERC CIP, NIST, AND DOE CYBERSECURITY 2 (2011), *available at* https://www.selinc.com/literature/TechnicalPapers. The reliability standard development process is a self-regulatory model by which the industry develops the standards that regulate it; however, FERC retains the final decision-making authority over whether or not to promulgate the standards. *Id.*

149. Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (portions relevant to this Note codified as amended in scattered sections of Title 16 of the United States Code.).

150. *See infra* Part V.A.1–2.

151. As noted previously, "defense needs to be strong everywhere, while the offense only needs to succeed in one place," and inconsistent security protocols run contrary to the coherent defense-in-depth strategy that is necessary. *See* Swire & Ahmad, *supra* note 78.

A. FERC, NERC, and the Mandatory Reliability Standard Development Process

Under section 215 of the EPAct,[152] Congress granted FERC the authority to develop mandatory standards aimed at ensuring the reliability of the "bulk-power system."[153] "Reliability standards" include requirements for "existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities."[154] The "bulk-power system" includes "facilities and control systems necessary for operating an interconnected electric energy transmission network" and "electric energy from generation facilities needed to maintain transmission system reliability."[155] Notably, the "bulk-power system" *excludes* "facilities used in the local distribution of electric energy."[156]

The statute further directed FERC to certify an "Electric Reliability Organization" (ERO) to "establish and enforce reliability standards for the bulk-power system, subject to [FERC] review."[157] In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the ERO. NERC's principal members are owners, operators, and users of the bulk-power system.[158] Once NERC has developed a reliability standard,[159] it submits it to FERC for approval. If FERC disapproves of a standard in whole or in part, it is not given statutory authority to unilaterally modify the standard;

---

152. Codified at 16 U.S.C. § 824o (2012).

153. *Id.*

154. § 824o(a)(3).

155. § 824o(a)(1)(A)–(B).

156. § 824o(a)(1).

157. § 824o(a)(2) & (c).

158. H.R. REP. NO. 111-493, at 9 (2010); *see also Key Players*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx (last visited Apr. 13, 2014) (indicating that the members of NERC's eight Regional Entities include "investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and end-use customers").

159. Approval of a reliability standard, or revision of an existing standard, requires two things: (1) a quorum of seventy-five percent of the member ballot pool, and (2) a two-thirds supermajority of the weighted segment of votes cast must be affirmative (the number of votes cast includes affirmative and negative votes, but excludes abstentions and non-responses). N. AM. ELEC. RELIABILITY CORP., STANDARD PROCESSES MANUAL 4–5 (2013), *available at* http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf. A reliability standard is initially drawn up by a "drafting team" comprised of industry experts appointed by the Standards Committee. *See id.* at 11. NERC uses a voting formula that "allocates each industry Segment an equal weight in determining the final outcome of any Reliability Standard action." *Id.* at 4.

however, it may remand the standard to NERC for further consideration.[160] FERC may also conduct formal rulemaking proceedings for submitted reliability standards to allow for comment by other interested parties.[161] Ultimately, to establish a mandatory reliability standard, FERC must determine that the standard, as filed, is "just, reasonable, not unduly discriminatory or preferential, and in the public interest."[162] Once approved by FERC, the reliability standard becomes mandatory for participants in the bulk-power system, and enforceable by NERC.[163]

NERC documentation has suggested that while interoperability standards operate to ensure free exchange of information in the Smart Grid without logical barriers, reliability standards put barriers in place to protect the critical infrastructure assets of the bulk power system.[164] It has also indicated that NERC's understanding of the mandate set forth under 16 U.S.C. § 824o places the focus of reliability standards more on physical aspects of the grid, including "installed equipment" and "the operation and maintenance of cyber assets."[165] Reliability standards shape the behavior of "asset owners and operators," not "equipment and system designers, manufacturers, and integrators."[166] Notably, NERC documentation indicates that NERC does not believe that reliability standards are intended to "specifically protect telecommunications systems or communications paths,"[167] underscoring the need for interoperability standards.

B. NIST and the Interoperability Standard Development Process

Under EISA,[168] NIST was given the "primary responsibility" of developing and coordinating a framework for "interoperability of smart grid devices and systems" that would "contribute to an

---

160. *See* § 824o(d)(4).

161. *See* DOLEZILEK & HUSSEY, *supra* note 148, at 2.

162. *See* § 824o(d)(2).

163. § 824o(e).

164. N. AM. ELEC. RELIABILITY CORP., COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0 (DRAFT) 10 (2009), *available at* http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20NIST/FinalNERCCommentsNIST_Smart_Grid_Framework_Document.pdf.

165. *Id.* at 11.

166. *Id.*

167. *Id.*

168. Relevant section codified at 42 U.S.C. § 17385 (2012).

efficient, reliable electricity network." Interoperability concerns the communication paths that exist between actors[169] along which they connect to "transmit, store, edit, and process the information needed within the Smart Grid."[170] Congress granted FERC the authority to review "work" prepared by NIST and, upon FERC's judgment that such work has led to "sufficient consensus," institute a "rulemaking proceeding to adopt . . . standards and protocols . . . necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[171] However, Congress did not define "work," "sufficient consensus," or "adopt." Also notably missing from the legislation was an enforceability provision.

In November 2009, NIST established the Smart Grid Interoperability Panel (SGIP) to coordinate the development of non-mandatory interoperability standards.[172] SGIP's members represent twenty-two Smart Grid stakeholder categories and "[a]ll seven integrated domains of the power system—customers, markets, service providers, operations, bulk generation, transmission, and distribution."[173]

---

169. "Actors" are devices, computer systems, software programs, the individuals, or organizations that participate in the Smart Grid. *See* NIST GUIDELINES VOL. 1, *supra* note 38, at 11.

170. *Id.* at 15.

171. § 17385(d).

172. *See* Joel B. Eisen, *Smart Regulation and Federalism for the Smart Grid*, 37 HARV. ENVTL. L. REV. 1, 38–39 (2013). For an interoperability standard to be approved and, thus, added to the "SGIP Catalog of Standards," there must be a "Governing Board recommendation and a vote by the SGIP members, with both votes requiring 75% in favor of approval." *Id.* at 39–40. In the end, while the Catalog of Standards is a "toolkit" for Smart Grid stakeholders, the approved standards are in no way mandatory. *Id.* at 42.

173. *See About Us*, SMART GRID INTEROPERABILITY PANEL, http://www.sgip.org/about_us/#sthash.GsJwOWVO.dpbs (last visited Apr. 13, 2014). The SGIP in turn established a permanent working group known as the Cybersecurity Working Group (CSWG), which has compiled some of the most substantial reports on Smart Grid cybersecurity, including three volumes of the "Guidelines for Smart Grid Cyber Security," referenced herein, and has the primary objective of "assess[ing] standards for applicability and interoperability across the domains of the Smart Grid." *See* NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS 2.0, at 142 (2012), *available at* http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf. In April 2013, SGIP fully transitioned into a "non-profit private-public partnership organization . . . supported by industry stakeholder funding and funding provided through a cooperative agreement with NIST." *Smart Grid Interoperability Panel*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/smartgrid/sgipbuffer.cfm (last visited Dec. 7, 2013). Prospective "participating" or "observing" members must now pay fees to join the new "SGIP 2.0, Inc."

NIST standards may only gain regulatory significance if they become part of a rulemaking proceeding by FERC under 42 U.S.C. § 17385(d).[174] Notably, though, EISA does not provide express authority to enforce interoperability standards created under the statute to either NIST or FERC, unlike the clear grant of enforcement authority for reliability standards under the EPAct.[175] FERC's position is that EISA did not grant it the authority to make or enforce mandatory interoperability standards.[176] As a result, to promulgate enforceable mandatory interoperability standards under the current EISA regime, FERC would have to reinterpret its own authority. Standards set forth after such a change in policy present an issue because they may be invalidated as "arbitrary and capricious" under the Administrative Procedure Act.[177]

FERC has interpreted its own authority under EISA as including adoption of standards that would "be applicable to all electric power facilities and devices with smart grid features, *including those at the local distribution level and those used directly by retail customers so long as the standard is necessary for the purpose [of 16 U.S.C. § 824o]*."[178] This interpretation represents a jurisdictional reach greater

---

Membership, SMART GRID INTEROPERABILITY PANEL, http://www.sgip.org/membership/#sthash.BRsKbeG2.dpbs (last visited Apr. 13, 2014).

174. § 17385(d).

175. *See* 16 U.S.C. § 824o(e) (2012) (detailing ERO authority in enforcing mandated reliability standards); Eisen, *supra* note 172, at 37 ("Critically, the EISA did not give FERC any new powers to enforce any standards it might adopt, beyond its existing FPA authorities to regulate interstate transmission of electricity. Its role is limited to ensuring the standards' functionality.").

176. Smart Grid Policy, 74 Fed. Reg. 37,098, 37,101 (July 27, 2009).

177. *See* 5 U.S.C. § 706(2)(A) (2012). A reviewing court shall "hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Id.* The Supreme Court has held that in order for a changed policy to survive "arbitrary and capricious" review, it suffices that (1) the new policy is permissible under the statute, (2) there are good reasons for it, and (3) the agency believes it to be better. *See* FCC v. Fox Television Stations, Inc., 556 U.S. 502, 515 (2009). However, a court may conduct a more searching review of the justifications for the change in policy if, for example, the new policy rests on facts that contradict those which underlay its prior policy, or if the prior policy engendered serious reliance interests. *Id.* at 516. In such a rapidly growing industry, there may be powerful reliance interests founded on FERC's prior policy; for example, significant investments made by businesses with the understanding that FERC would not mandate enforceable communication security standards may prove financially detrimental should their systems be found noncompliant with new enforceable standards and in need of substantial retooling. Those reliance interests arguably become stronger as time progresses.

178. Smart Grid Policy, 74 Fed. Reg. 37,098 (emphasis added).

than the one in the reliability sphere.[179] FERC's position met with significant opposition from members of the electricity industry and PUCs.[180] Industry members asserted that technical standards are typically developed and adopted by the private sector on a voluntary basis, while PUCs claimed that they retained jurisdiction over distribution-level projects.[181] One argument set forth by utilities and PUCs in protecting their activities from mandated technical requirements was that "mandated standards preserve technologies in amber, making them potentially obsolete later."[182]

These statutory ambiguities and jurisdictional conflicts have led to a stalemate: to date, FERC has not mandated any technical interoperability standards. NIST only made one attempt to submit standards to FERC for consideration in a potential rulemaking proceeding. On October 6, 2010, NIST notified FERC that it had "identified five families of standards as ready for consideration by regulators."[183] Ultimately, FERC issued an order on July 19, 2011 finding that there was "insufficient consensus" to institute a rulemaking proceeding on the five families of standards.[184] Since then, no other standards have been submitted to FERC by NIST. However, NIST has continued to develop voluntary standards and prepare comprehensive reports analyzing, in great detail, the many communication interfaces existing within the Smart Grid and offering suggestions on how to enhance their security. In fact, *fifty-six voluntary standards* have been approved through the SGIP process,[185] and subsequently added to SGIP's Catalog of Standards.[186]

The security deficiencies that can arise from reliance upon voluntary standards were illuminated in a report developed by Congressmen Edward J. Markey and Henry A. Waxman, then-Chairman of the House Subcommittee on Energy and Environment

---

179. Regulatory jurisdiction in the reliability sphere reaches the "bulk-power system," which includes generational and transmission facilities, but *excludes* facilities used in the local distribution of electric energy. *See supra* notes 152–56 and accompanying text.

180. *See* Eisen, *supra* note 172, at 51.

181. *See id.*

182. *Id.*

183. FERC Order on Smart Grid Interoperability Standards, 136 F.E.R.C. 61,039, Slip Op. at 3 (July 19, 2011), *available at* http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf.

184. *Id.* at i. For a deeper discussion of FERC's order, see *infra* Part V.A.1.

185. *See supra* note 172 and accompanying text for a description of the process.

186. *SGIP Catalog of Standards Information Library*, NAT'L INST. STANDARDS & TECH., http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCoSStandardsInformationLibrary (last visited Apr. 13, 2014).

and then-Chairman of the House Energy and Commerce Committee, respectively. The report identifies both mandatory and voluntary NERC standards[187] and polled utilities about their compliance with each.[188] The Senators found that most utilities only comply with mandatory cybersecurity standards, without implementing voluntary NERC recommendations.[189]

The utilities' failure to implement adequate cybersecurity standards is also demonstrated in another report prepared by the DOE's Inspector General, which showed that while ninety-nine grants were awarded by the DOE under its "Smart Grid Investment Grant" (SGIG) program totaling $7.8 billion,[190] thirty-six percent of grant applications "were missing at least one of the required cyber security elements."[191] The report concluded that the approved cybersecurity plans did not adequately address security risks or planned cybersecurity controls.[192]

EISA's lack of an enforcement provision in conjunction with FERC's disclaimer of authority to promulgate mandatory enforceable interoperability standards has resulted in a voluntary adoption regime.[193] Congressmen Markey and Waxman's report demonstrated that utilities implemented voluntary standards less often than mandatory ones. The DOE Inspector General's report showed inadequate cybersecurity planning by recipients of SGIG grants. These facts reveal some of the potential flaws of a voluntary regime.

---

187. It is worth noting that these standards were aimed at reducing vulnerabilities identified by analysis of the Stuxnet and Aurora occurrences, discussed *supra* Part II.A.

188. *See* MARKEY REPORT, *supra* note 87, at 12.

189. *Id.* For example, 91% of investor-owned utilities, 83% of municipally- or cooperatively-owned utilities, and 80% of federal entities that own major pieces of the bulk-power system reported compliance with the mandatory Stuxnet standards, while 21% of investor-owned utilities, 44% of municipally- or cooperatively-owned utilities, and 62.5% of federal entities reported compliance with the voluntary Stuxnet standards.

190. *See* Paladino, *supra* note 51.

191. *See U.S. Smart Grid Projects Failing on Security*, INFORMATION AGE (Jan. 27), 2012, http://www.information-age.com/technology/information-management/1687918/us-smart-grid-projects-failing-on-security.

192. *Id.*

193. Pursuant to a performance audit of electrical grid cybersecurity, the United States Government Accountability Office concluded that FERC's lack of enforcement authority rendered standards developed by NIST under EISA voluntary. U.S. GOV'T ACCOUNTABILITY OFFICE, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 18 (2011), *available at* http://www.gao.gov/new.items/d11117.pdf.

C. Subsequent Legislative and Executive Efforts to Address Electric Grid Cybersecurity, and the Likelihood of Successful Future Legislation

Since their passage, it has become apparent that neither EPAct nor EISA grant federal agencies the authority necessary to protect the electrical grid from cyber threats. High-level FERC officials have cited cybersecurity as the top threat to the nation's electric grid and encouraged—and at times implored—Congress to provide a federal body with sufficient enforcement authority to secure the grid.[194] Legislation aimed at addressing cybersecurity shortcomings in different ways has been proposed, with some bills coming closer to enactment than others.

The electrical grid cybersecurity bill that came closest to enactment was introduced in the House of Representatives on April 14, 2010 as H.R. 5026, also known as the Grid Reliability and Infrastructure Defense Act (GRID Act).[195] The GRID Act would have granted FERC the authority to issue emergency orders to protect the grid against a security threat brought to its attention by the President. FERC would have also been authorized to promulgate a rule or issue an order, independent of NERC, requiring owners and operators in the bulk-power system[196] to implement measures to protect against any grid security vulnerability that had not been adequately addressed by NERC-developed reliability standards. The bill was

---

194. In 2011, all five FERC commissioners indicated at a House of Representatives hearing that they considered a cyber attack on the electrical grid as the top threat to electric reliability, and several emphasized the need for additional enforcement authority. *See The American Energy Initiative, Part 12: Impacts of the Environmental Protection Agency's New and Proposed Power Sector Regulations on Electric Reliability: Hearing Before the H. Subcomm. on Energy and Power of the H. Comm. On Energy and Commerce*, 112th Cong. 251–52 (2011). In 2012, FERC Chairman Jon Wellinghoff implored Congress to empower a federal body with the powers necessary to protect the grid from cyber threats. Chairman Wellinghoff stated that FERC had (1) no effective way to confidentially communicate cyber threats to utilities, and (2) no effective enforcement authority, adding, "I don't care who has the authority, just give it to somebody so we can do something. The Congress should give someone the authority." Darius Dixon, *FERC Chief Says Power Grid Lacks Cybersecurity Mandate*, U.S. SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFF. (Sept. 6, 2012), http://www.hsgac.senate.gov/media/ferc-chairman-says-electric-grid-natural-gas-lines-are-vulnerable-to-cyber-attack-.

195. *See* S. COMM. ON ENERGY AND NATURAL RES., 111TH CONG., LEGISLATIVE CALENDAR ONE HUNDRED ELEVENTH CONGRESS 2009–2010, at 81–82 (2010).

196. The GRID Act retained the definition of the bulk-power system from section 215 of the FPA, which excluded distribution level facilities. *See* H.R. 5026, 111th Cong. § 215A(a)(1) (2010) (adopting the definition of the bulk-power system given in § 215(a) of the Federal Power Act, codified at 16 U.S.C. § 824o(a)(1) (2012)).

reported to the house by a 47–0 vote of the House Committee on Energy and Commerce on May 25, 2010. The House of Representatives passed H.R. 5026 on June 9, 2010. It was then referred to the Senate Energy and Natural Resources Committee on June 10, 2010, where it was ultimately reported out to the Senate with an amendment in the nature of a substitute bill[197] and placed on the Senate Legislative Calendar on September 27, 2010. The bill never made it to the Senate floor.

Regarding H.R. 5026's failure in the Senate, Congressman Edward Markey, a co-sponsor of the original House version of the bill, believed that the "electric utility industry . . . successfully persuaded Senate Republicans to stall the bill" and had "lobbied aggressively against the measure. House Republicans have acceded to industry's desire to simply regulate itself."[198] At a House hearing in 2011, two congressmen indicated that the difficulty in the Senate was not *whether* additional legislation addressing the grid's cybersecurity shortcomings should be passed, but *how* those shortcomings should be addressed.[199] Other legislative efforts of varying success over the

---

197. Notably, the substitute bill would have expanded FERC's jurisdiction beyond the bulk-power system to include "systems and assets . . . used for . . . distribution of electric energy affecting interstate commerce . . . ." S. REP. NO. 111-331, at 1 (2010). Similar to H.R. 5026, it would have authorized FERC to issue its own rules or orders without prior notice or hearing to protect the grid from cybersecurity vulnerability. However, the substitute removed aspects of H.R. 5026 that addressed threats to the grid by electromagnetic pulses and solar flares. *See id.*; *see also* Ken Timmerman, *Murkowski Blocks Effort to Protect US Power Grid,* NEWSMAX (Oct. 14, 2010), http://www.newsmax.com/KenTimmerman/lisa-murkowski-emp-energy/2010/10/14/id/373768.

198. Letter from Edward J. Markey, U.S. Representative of Mass., to Barack Obama, President of the United States (Aug. 8, 2012), *available at* http://democrats.naturalresources.house.gov/sites/democrats.naturalresources.house.gov/files/documents/2012-08-08_GridSecurity_POTUS.pdf. Utility industry reticence may be, at least in part, attributable to the industry's belief that it is already subjected to ample mandatory cybersecurity regulations. The American Public Power Association noted that "[u]nlike other industry sectors, the electric utility industry must comply with an extensive list of mandatory reliability standards, including cybersecurity standards." AM. PUB. POWER ASSOC., STATEMENT BY THE AMERICAN PUBLIC POWER ASSOCIATION ON 10TH ANNIVERSARY OF 2003 NORTHEAST BLACKOUT (2013), *available at* http://www.publicpower.org (follow "Resources" hyperlink; then follow "Archived press releases" hyperlink; then follow "8/15/2013" hyperlink).

199. Congressman Trent Franks of Arizona stated that the "big challenge was that [Senators] had differing strategies on what should be done about cybersecurity." *Protecting the Electric Grid: H.R. ___, the Grid Reliability and Infrastructure Defense Act: Hearing Before the H. Subcomm. on Energy and Power of the H. Comm. On Energy and Commerce*, 112th Cong. 49 (2011) (statement of Trent Franks, U.S. Rep. of Ariz.). Congressman James R. Langevin added, "[W]e were a bit frustrated by the Senate still contemplating which path forward they were going to

past five years have shown that while Congress is cognizant of the importance of filling regulatory gaps to ensure Smart Grid cybersecurity, it has had difficulty finding the right mix of provisions that would allow legislation to pass both Houses.[200]

In the absence of new legislation, President Obama issued an executive order on February 12, 2013 entitled "Improving Critical Infrastructure Cybersecurity."[201] The order emphasized collaboration between the United States government and critical infrastructure owners and operators.[202] It also reinforced the importance of NIST's role in developing a "Cybersecurity Framework" to reduce cyber risks to critical infrastructure, incorporating voluntary consensus standards and industry best practices.[203] The Secretary of Homeland Security was ordered to establish a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure," as well as incentives designed to promote participation in the program.[204] The President's order therefore sustained the voluntary interoperability standard adoption environment that has persisted following the passage of EPAct and EISA, with an eventual aim of incentivizing adoption.

---

take," with the key to achieving Senate cooperation being "perseverance." *Id.* at 49–50 (statement of James R. Langevin, U.S. Rep. of R.I.).

200. H.R. 668, also known as the Secure High-voltage Infrastructure for Electricity from Lethal Damage Act, or "SHIELD Act," focused on the protection of the grid from damage by geomagnetic storms or electromagnetic pulses, which was one area of focus in the GRID Act as well; however, it does not address the other important component of the GRID Act—electronic communication-based cyber threats. *See* H.R. 668, 112th Cong. (2011). The bill was not reported out of the Committee on Energy and Commerce in 2011, but was reintroduced as H.R. 2417 on June 18, 2013 and referred to the same committee. *See H.R. 668 (112th): Secure High-voltage Infrastructure for Electricity from Lethal Damage Act*, GOVTRACK, https://www.govtrack.us/congress/bills/112/hr668 (last visited Apr. 13, 2014). S. 1342, also known as the Grid Cyber Security Act, would have expanded FERC's jurisdiction in instituting reliability standards to include distribution-level facilities and authorized FERC to direct NERC to develop and implement mandatory cybersecurity standards, rather than having to wait for NERC to bring it standards for approval. *See* S. 1342, 112th Cong. §§ 215(d)(7), 224(a)(1) (2011). This was a retreat from the GRID Act, which sought to authorize FERC to promulgate cybersecurity rules or standards independent of NERC under certain circumstances. *See* H.R. 5026, 111th Cong. § 215A(b)–(c) (2010). The bill was reported out of the Senate Committee on Energy and Natural Resources, but saw no further congressional action. *See S. 1342 Bill Summary & Status*, LIBRARY CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN01342:@@@X (last visited Apr. 13, 2014).

201. Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

202. *See id.*

203. *See id.* at 11,740–41.

204. *See id.* at 11,741–42.

While developing an effective incentive-based voluntary environment sounds attractive in some ways, it is important to note that it may take significant time to identify appropriate incentives and then perfect the incentive program through periods of trial-and-error. Given the rapid pace at which the Smart Grid is developing[205] and the time that has elapsed thus far without FERC adopting interoperability standards under EISA,[206] this planning and implementation window may render the grid vulnerable in the meantime with information technology ultimately becoming so entrenched that achieving retroactive compliance would be extremely costly and time-consuming. Through a performance audit, the Government Accountability Office found that while some grid stakeholders believed that "economic and market pressure should encourage manufacturers and utilities to follow voluntary standards," others felt there could be gaps in compliance where there are significant cost considerations, or simply unfamiliarity or disinterest in implementation.[207]

In assessing whether Smart Grid interoperability standards should remain free from government mandates and left to the electricity industry members to develop, implement, and possibly enforce, consideration of an existing industry-created and policed standard regime, such as the Payment Card Industry Data Security Standard (PCI-DSS), can provide insight as to how fitting such a regime might be for the future of the Smart Grid.

IV. THE PROBLEMS THAT ARISE FROM VOLUNTARY STANDARDS: PCI-DSS AS AN INDUSTRY-DEVELOPED STANDARD ANALOGUE

Some have suggested that voluntary industry-developed interoperability standards would allow for the effective market-driven evolution of the Smart Grid industry, similar to the growth of the Internet[208] which, in the 1990s, Congress found presented a "forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity"

---

205. *See infra* note 246 and accompanying text.

206. *See infra* note 239 and accompanying text.

207. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 193.

208. *See* Eisen, *supra* note 172, at 55–56. The utility industry has lobbied against additional federal authority to mandate cybersecurity standards, seeking instead to regulate itself. *See* Letter from Edward J. Markey, *supra* note 198.

that flourished with a minimum of government regulation.[209] The payment card industry is another example of a sector that has, to a large extent, regulated itself through an industry-developed standard: PCI-DSS. This standard does have enforcement elements, but is voluntary in the sense that it is enforced through private agreements rather than government mandates.[210] While PCI-DSS has not been a complete failure, it has had its share of cybersecurity challenges.[211] PCI-DSS shows that even where there are creative industry-developed standards and enforcement procedures, substantial breaches will still occur. The risk of noncompliance is even greater where, as in the Smart Grid, the voluntary standard regime lacks private enforcement procedures.

PCI-DSS is a security standard in the United States that applies to the payment card industry. The standard is established by a consortium of the major credit card companies in the United States[212] and requires that merchants accepting credit card payments implement the standard, which is designed to provide an "actionable framework for developing a robust payment card data security process—including prevention, detection and appropriate reaction to security incidents."[213] Although the standard is developed cooperatively, each card brand has its own requirements that merchants accepting that brand must meet.[214] It is an industry-developed and industry-enforced standard aimed at protecting cardholder data[215] and represents a form of "private ordering" by which behavior and resolution of disputes are regulated by non-

---

209. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (citing congressional findings codified at 47 U.S.C. § 230(a)(3) (2012) pursuant to the passage of the Communications Decency Act of 1996).

210. *See* Edward A. Morse & Vasant Raval, *Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 231 (2012).

211. *See infra* notes 218–24 and accompanying text.

212. The credit card consortium includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. *What Is the PCI Security Standards Council?*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/role_of_pci_council.php (last visited Apr. 13, 2014).

213. *PCI SCC Data Security Standards Overview*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/index.php (last visited Apr. 13, 2014).

214. The payment card brands place merchants in various tier systems based on volume of transactions, with merchants conducting more transactions being subjected to more stringent security requirements. *See* Morse & Raval, *supra* note 210, at 235–37.

215. *See* VERIZON, *supra* note 104, at 56.

governmental entities.[216] The standards are rooted in the economic benefits the payment card industry realizes from easing consumer fears regarding unauthorized charges that may otherwise discourage them from using payment cards.[217]

One report analyzed breaches of organizations required to comply with PCI-DSS.[218] It highlighted the problem of the "comparative mindset" in implementing an information technology security strategy: organizations rationalize that "being just slightly better than others also somehow equates to being secure."[219] Where there is total freedom, i.e., in the absence of mandatory standards, the comparative mindset may result in organizations settling for especially low levels of security.

The report identified three comparative mindset categories: good, better, and best.[220] A "good" security mindset is "my security is better than [that of] many of my peers, but we're still not meeting our compliance requirements;" a "better" mindset is "my security is better than [that of] most of my peers and also meets the *letter* of our compliance requirements;" the "best" mindset is "my security is better than [that of] most of my peers, meets the spirit of our compliance requirements, and evolves with the changing threat landscape."[221] The report found that ninety-six percent of organizations subject to PCI-DSS that had been breached were non-compliant, failing to display the "better" or "best" mindsets. The majority of breach victims did not even make the "good" security category.[222] This shows that even in a system governed by an "extralegal mechanism with an elaborate set of processes, structures, and information,"[223] and fine structures aimed at incentivizing security investment, non-compliance is still a significant issue.[224] In the Smart Grid, the lack of enforceable penalties only amplifies these non-compliance concerns.

---

216. Morse & Raval, *supra* note 213, at 214.

217. *See id.* at 223–24 (noting that payment card firms offer consumers more protection than is mandated under federal law, with "[s]elf-interest produc[ing] this result: if consumer fears regarding unauthorized charges induce them not to use their cards, the payment card industry makes no profits").

218. *See* VERIZON, *supra* note 104, at 56–60.

219. *See id.* at 56.

220. *Id.*

221. *See id.*

222. *See id.*

223. Morse & Ravel, *supra* note 210, at 237.

224. *See* VERIZON, *supra* note 104, at 2.

Private ordering without significant government intervention may be appropriate in some circumstances. Maybe there is a gap in technical expertise between private businesses and public regulators that would render public efforts to intervene critically uninformed and ineffective. As in the case of PCI-DSS, it might be that industry standards imposed through contracts can be sufficiently driven by economic incentives.[225] Perhaps there is a greater overarching governmental interest that justifies a more "hands-off" approach, such as nurturing a burgeoning forum for discourse and cultural development like the Internet.[226]

In the Smart Grid context, however, NIST has established itself as an agency with significant expertise.[227] Additionally, it is unclear whether Smart Grid industry participants will realize the same type of economic benefits of security so that they will privately order themselves, through contractual arrangements, in a manner that will allow for the type of industry-enforced standards present in PCI-DSS. Congress has expressed that it is United States policy to modernize the electrical grid to "maintain a reliable and *secure* electricity infrastructure," through, in part, the "[d]ynamic optimization of grid operations and resources, with *full cyber-security*."[228] Whereas freedom of speech and expression were primary concerns in regulating the Internet, ensuring full critical infrastructure cybersecurity—and thus national security—should be a primary concern in the Smart Grid.

V. SHAPING A SOLUTION

Private ordering is not a strong option for the Smart Grid because there is a weak "expertise gap" argument, uncertain economic incentives for implementing interoperability security, and a congressional commitment to obtaining full Smart Grid cybersecurity. Part V.A demonstrates that the inadequacy of the current system, the high stakes involved, and the expertise and experience of NIST render federal mandatory enforceable standards governing the communication of information in the Smart Grid the most appropriate response to ensure Smart Grid cybersecurity. Part V.B explains why NIST is the appropriate entity to be given the authority

225. *See supra* note 217 and accompanying text.
226. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).
227. *See infra* Part V.B.2.
228. 42 U.S.C. § 17381(2) (2012) (emphasis added).

to do so, while describing what a legislative solution in this spirit might look like.

A. Mandatory Federal Standards Governing Smart Grid Information Systems Are Necessary

It can be argued that a blossoming industry centered on new technologies (e.g., the Internet) may, in some circumstances and in light of certain goals, be better served by an unregulated environment.[229] Nevertheless, given that the developing Smart Grid industry is grounded in and developing upon the generation, transmission, distribution, and consumption of electricity, important interests are raised that render mandatory regulations more appropriate.[230] This subpart will explore three justifications for mandatory federal regulation of Smart Grid information systems: (1) the inadequacy of the current system, (2) the high stakes involved, and (3) the benefits to all stakeholders of a uniform standard approach.

1. The Current System for Development of Interoperability Standards Is Inadequate

Currently under EISA, FERC is instructed to institute a rulemaking proceeding to adopt interoperability standards developed by NIST once FERC has determined that such standards have reached "sufficient consensus."[231]

This process has only been explored once when NIST submitted a letter to FERC on October 6, 2010, indicating that it had "identified five foundational families of standards as ready for consideration by regulators."[232] On July 19, 2011—more than nine months later—FERC issued an order refusing to initiate a rulemaking proceeding in

---

229. *See supra* note 209 and accompanying text. Professor Joel B. Eisen has suggested that allowing the Smart Grid to evolve in a manner similar to the Internet would "yield better results than trying to dictate mandatory standards today." *See* Eisen, *supra* note 172, at 56.

230. *Cf.* NIST GUIDELINES VOL. 1, *supra* note 38, at 76 ("Power system operations pose many security challenges that are different from most other industries. For example, the Internet is different from the power system operations environment. In particular, there are strict performance and reliability requirements that are needed by power system operations.").

231. *See supra* note 171 and accompanying text.

232. Letter from George Arnold, Nat'l Coordinator, Smart Grid Interoperability, to Jon Wellinghoff, Chairman, Fed. Energy Regulatory Comm'n (Oct. 6, 2010), *available at* http://www.nist.gov/public_affairs/releases/upload/FERC-letter-10-6-2010.pdf.

connection with these five families of standards.[233] Ironically, FERC cited concerns that the proposed cybersecurity standards may lead to cybersecurity deficiencies.[234] FERC explained that while, at the time of the order, the "NIST interoperability framework process" was the "best vehicle for developing smart grid interoperability standards," certain aspects of that process were not in place at the time the proposed standards were being developed,[235] which contributed to the finding of insufficient consensus. The order concluded by giving NIST and SGIP supportive praise, encouraging "utilities, smart grid product manufacturers, regulators, and other smart grid stakeholders to actively participate in the NIST interoperability framework process."[236]

SGIP responded to FERC's decision by stating that it "appreciate[d]" FERC's acknowledgment of SGIP's value,[237] and George Arnold, the Smart Grid National Coordinator for NIST, stated that NIST supported FERC's order.[238] Despite NIST and SGIP's continuing development of impressive work product aimed at encouraging Smart Grid cybersecurity, the EISA rulemaking procedure has not been pursued again since it failed in July 2011. Thus, in the almost *six years* since EISA created this interagency coordination procedure, FERC has not promulgated any interoperability standards or protocols, despite projections that Smart Meters will be installed in over half the nation's homes by 2015.[239]

Even if rules had been established, it is unclear from the language of EISA what enforcement tools FERC would have had at its disposal to enforce them. FERC has reinforced the enforcement predicament by issuing a notice indicating that it did not interpret EISA as

---

233. *See* FERC Order on Smart Grid Interoperability Standards, *supra* note 183.

234. FERC explained that the standards were not adopted in part because "[c]ommenters were nearly unanimous" in their opposition to the standards, "citing concerns with cyber security deficiencies and potential unintended consequences from premature adoption of individual standards." *Id.* at 5.

235. *Id.*

236. *Id.* at 7.

237. *See FERC Will Not Adopt Five NIST-Recommended Smart Grid Standards*, ELECTRIC LIGHT & POWER (July 27, 2011), http://www.elp.com/articles/2011/07/ferc-will-not-adopt-five-nist-recommended-smart-grid-standards-.html.

238. Mr. Arnold stated that the order was "consistent with NIST's public comments to the commission that it can send appropriate signals to the marketplace by recommending use of the NIST framework and that it would be impractical and unnecessary for the commission to adopt individual interoperability standards." Michael Bates, *FERC Decision Leaves Grid Interoperability Standards in Limbo*, RENEW GRID (July 21, 2011), http://www.renewgridmag.com/e107_plugins/content/content.php?content.7062.

239. *See supra* note 44 and accompanying text.

granting it the authority to promulgate enforceable mandatory standards, meaning that, under the existing regime, FERC would have to first reinterpret its own authority, which could prove challenging.[240]

Given that SGIP requires a seventy-five percent approval rate before adding an interoperability standard to its Catalog of Standards,[241] to *also* require a finding of undefined "sufficient consensus" by FERC after SGIP has blessed the standard by such a significant supermajority of diverse Smart Grid stakeholders[242] can take a long time, is redundant, and is ultimately a very high barrier to the promulgation of interoperability standards.

The push for adoption of voluntary standards often relies upon the "hortatory ability" of government agencies such as NIST, DOE, and FERC in convincing stakeholders and PUCs that standards should be followed.[243] Without mandatory enforceable requirements, the decision might simply come down to whether cybersecurity is a "reasonable and prudent" investment.[244] Although the development of mandatory reliability standards by NERC and FERC under the EPAct are necessary to ensure that the critical assets of the Smart Grid are secured, the communications between these components must be secured as well.[245] This goal should be accomplished through similarly mandatory and enforceable interoperability standards. The failure to promulgate any interoperability standards since the inception of EISA in 2007, the absence of an express statutory grant of enforcement mechanisms, and the redundancy of a double-consensus system involving undefined requirements (e.g., "sufficient consensus") indicate an unacceptable level of inactivity in a burgeoning industry,[246] given the high stakes.

---

240. *See supra* notes 176–77 and accompanying text.

241. *See supra* note 172 and accompanying text.

242. For a description of SGIP participants, see *supra* note 173 and accompanying text.

243. *See* Ray Gifford & Eric Gunning, *The Opportunity and Peril of Smart Grid*, 11 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 128, 129 (2010).

244. *Id.* at 130.

245. While NERC and FERC reliability standards may aid in securing the components that make up the Smart Grid, "[t]he strongest adversaries are not going to waste time attacking a component device that is known to be a fortress." Instead, attackers will look to find weaknesses between the secure components as they speak to each other and communicate information. *See* PIKE RESEARCH, *supra* note 76, at 6–7.

246. The Institute for Electric Efficiency found that while Smart Meters were installed in approximately one-in-four homes as of September 2011, their presence in

2. The High Stakes Nature of an Industry Based on the Nation's Electric Grid Warrants Mandatory Enforceable Federal Standards

Time is of the essence. The deployment of technology in distribution-level equipment, generation facilities, utilities, and ESPs in the absence of interoperability standards will result in security that is only as strong as individual companies choose to make it. Even if a company chooses to make cybersecurity a top priority, information may become vulnerable at some point as it travels through communication pathways between other less-secure entities, given the lack of a uniform standard by which all parties participating in that type of communication must abide. Those vulnerabilities only proliferate as more equipment and technology is deployed in the absence of mandatory standards.

Electricity is ingrained in our daily lives.[247] The Department of Energy has stated that there is "the potential for extreme damage from a cyber attack"[248] on the electric grid that could cause "extended power outages and destruction of electrical equipment."[249] It added that a cyber attack could be "launched through the public network from a remote location anywhere in the world and could be coordinated to attack many locations simultaneously," and "[a]ny prolonged or widespread disruption of energy supplies could produce devastating human and economic consequences."[250] Consistent with the fact that we are dependent on electricity in virtually all aspects of our lives, a 2012 report prepared by industry experts assembled by the National Research Council stated that it is "no stretch of the imagination" to think that a "systematically designed and executed terrorist attack" could entail costs of hundreds of billions of dollars.[251]

---

over half of the nation's households is expected by 2015. *See* INST. FOR ELEC. EFFICIENCY, *supra* note 44.

247. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 19, at 5 (noting that "[m]odern society has come to depend on reliable electricity as an essential resource for national security; health and welfare; communications; finance; transportation; food and water supply; heating, cooling, and lighting; computers and electronics; commercial enterprise; and even entertainment and leisure").

248. *See* OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 53, at 3.

249. *Id.* at 1.

250. *Id.*

251. COMM. ON ENHANCING THE ROBUSTNESS & RESILIENCE OF FUTURE ELEC. TRANSMISSION & DISTRIBUTION IN THE U.S. TO TERRORIST ATTACK ET AL., TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM 1 (2012), *available at* http://www.nap.edu/catalog.php?record_id=12050. By way of comparison, the August 14, 2003 Northeast blackout, which affected approximately 50 million people and lasted up to four days in some areas, cost the United States between $4 billion and $10 billion. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, *supra* note 19, at 1.

One economist who produces security-related data for the government estimated that if one-third of the country lost power for three months it would cost the economy *$700 billion*, equivalent to "40 to 50 large hurricanes striking all at once . . . . [and] greater economic damage than any modern economy ever suffered."[252]

Two scholars highlighted the terror that might ensue in cities following targeted cyber attacks. They described the hypothetical scene in New York City following an anonymous attack aimed at disrupting the subway system, stranding subway cars in tunnels at 8:00 a.m. on a Thursday morning.[253] All systems that rely on electricity could be susceptible to Internet-based attacks on an enormous scale given the interconnected nature of the electrical grid. Adding to these significant communal and national security concerns are the substantial personal privacy concerns previously discussed.[254]

Given the inextricable integration of electricity in our daily lives, the rapidity with which the Smart Grid is developing, the national security and personal privacy and safety threats that infiltration of the Smart Grid through the Internet poses, and the enormity of the potential economic consequences, it is clear that too much is at stake to let Smart Grid stakeholders privately order themselves in the way that Internet stakeholders were permitted to. The integrity of the system must be the top priority where, as here, the threats are real, attacks have been committed, and many parties have an interest in capitalizing on vulnerabilities in the system.[255] This is a situation that calls for uniform mandated enforceable security requirements.

3. A Uniform Federal Approach to Cybersecurity Would Benefit All Smart Grid Stakeholders

State governments retained substantial regulatory control over utilities in the Traditional Grid.[256] Accordingly, state PUCs continue to assert their jurisdictional claim to distribution-level activities,

---

252. Meserve, *supra* note 81 (quoting economist Scott Borg).

253. *See* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1, 14-17. For another example of the frightening ripple effect "layered" cyber attacks might have, see *id.* at 23–24.

254. *See supra* Part II.C.

255. *See supra* Part II.A–B.

256. *See supra* Part I.A.2 (discussing the compact between states and utilities through which states gained regulatory authority over utilities in the Traditional Grid).

rebuffing the idea of federal regulation.[257] The resulting patchwork of state standards can lead to detrimental inconsistencies in an industry that has become interstate in nature.[258] As one such interstate industry, the Smart Grid would be better served by uniform federal standards.

First, a uniform set of mandatory interoperability standards would assist businesses by providing a set of rules to which innovations can be tailored. This solution would allow technologies to take root and develop reputations and track records. Utilities would likely be more comfortable adopting established technologies that have a lower likelihood of becoming obsolete or growing out of favor tomorrow.[259] Currently, Smart Grid businesses have likely been impacted in their decision-making by the uncertainty regarding interoperability standards. As one research report noted, "Those who choose to plow ahead now risk losing their entire investment if future laws invalidate their approach."[260] As the industry expands, more and more decisions are predicated on guesswork. The time to institute mandatory standards is now, rather than five years from now after there has been a cyber attack or new laws require the costly replacement of

---

257. *See, e.g.*, Bruce W. Radford, *The Smart-Enough Grid*, PUB. UTIL. FORTNIGHTLY (Aug. 2009), http://www.fortnightly.com/fortnightly/2009/08/smart-enough-grid (citing the California PUC as insisting that the states, rather than FERC, should have the authority to direct electric companies whether to institute NIST-developed standards at the distribution level); *see also supra* notes 180–82 and accompanying text.

258. *See, e.g.*, Morse & Raval, *supra* note 210, at 244 (highlighting the issues presented by a patchwork of state standards in the payment card industry by noting that "[v]ariation in requirements among the states potentially creates significant problems for firms engaged in multijurisdictional business operations, which might be solved by uniform requirements within a federal statute"). One scholar has noted that state-by-state Smart Grid solutions raise a number of issues, including unpredictable results and confusing implications for utilities that purvey electricity in more than one state. *See* Balough, *supra* note 124, at 183, 188–89. Even some PUCs, despite their opposition to a perceived federal usurpation of traditional state powers, have recognized that a "patchwork" of state standards could be harmful, *see* Radford, *supra* note 257 (citing statements by the California PUC), and that cybersecurity may be a special area over which federal regulatory authority is be appropriate, *see* Eisen, *supra* note 172, at 55 n.344 (noting that Michigan Public Service Commission opposed enforceable federal interoperability standards, except in limited areas, such as cybersecurity).

259. Given the nature of utilities as natural monopolies and the resulting regulatory environment, utilities seek to earn a negotiated return on prudent capital investments. Minimizing risk is a top priority, and "utilities are often slow to adopt new technologies that have not been extensively proven outside a laboratory." *See* Quinn & Reed, *supra* note 33, at 873.

260. *See* PIKE RESEARCH, *supra* note 76, at 5.

entrenched systems deemed non-compliant. These concerns only become more considerable with the passage of time.

Next, and most importantly, uniform mandatory standards would reduce the system vulnerabilities that result from voluntary standards where businesses have the option to invest a lot, a little, or nothing at all in cybersecurity.[261] If a critical piece of information flows through Companies 1, 2, and 3, with Companies 1 and 3 employing strong security measures and Company 2 employing weak security measures, the weakest link causes that information to become vulnerable to interception despite the efforts of Companies 1 and 3.[262] Uniform standards would help to ensure that information travels with a consistent level of protection throughout the Smart Grid,[263] protecting business operations from harmful intrusion and consumers from unwanted exposure of private information.

Finally, federal mandatory standards applicable to all Smart Grid stakeholders would provide certainty to an industry in which key players are risk-averse (i.e., electric utilities) by providing a firm footing upon which technologies can be built with a focused aim towards compliance. Creating uniform standards throughout the system would help to ensure fairness and reduce the likelihood that malicious parties would intercept information or access critical systems by exploiting a weak point in the network.

B. NIST Should Be Given Statutory Responsibility and Authority to Establish Mandatory Federal Standards that Apply to All Smart Grid Participants

A legislative solution reconfiguring and redefining responsibilities in a manner that removes FERC from the process and grants NIST

---

261. *See* generally *supra* Parts III.B, IV.

262. *See, e.g.*, PIKE RESEARCH, *supra* note 76, at 6–7 (noting that "[s]ecurity is only as strong as its weakest link and the best attackers know instinctively to look for that weak link," "[t]he best encryption algorithm in the world is useless if key distribution is not adequately secured," and "sophisticated attackers will look for holes in between secure components—things that architecture would address").

263. In explaining the rationale behind establishing a uniform approach to securing information in the federal system under its Federal Information Security Management Act powers, NIST stated that "[a] common foundation for information security will provide the Civil, Defense, and Intelligence sectors of the federal government and their support contractors, more cost-effective and consistent ways to manage information security-related risk to organizational operations and assets, individuals, other organizations, and the Nation." NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMM., NIST SPECIAL PUBLICATION 800-53, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, at vii (2013).

the authority to institute mandatory enforceable interoperability standards for all Smart Grid participants would require two essential determinations: (1) that federal regulatory jurisdiction in this manner is constitutional, and (2) that NIST is the appropriate federal entity to promulgate these standards. Several substantive and logistical considerations are also important to such a solution, including enforcement authority, industry involvement, compliance certification, and the ability of the standards to evolve over time.

1. Federal Jurisdiction Over All Smart Grid Participants is Appropriate

Although much of the regulation in the Traditional Grid was performed by state PUCs as part of the natural monopoly "compact" with utility companies,[264] the expansion of interstate transmission of electricity has substantially increased the reach of federal regulatory jurisdiction.[265] The Supreme Court has held that "any electricity that enters the grid immediately becomes a part of a vast pool of energy that is constantly moving in interstate commerce."[266] This modern understanding of the physical properties of electricity flowing in an interstate electrical grid counters the outdated perception that electricity provision is a localized operation best regulated by individual states.[267] Rather, it suggests that broader federal regulatory jurisdiction may be appropriate.

State PUCs have opposed FERC interpreting its authority under EISA to extend to "all electric power facilities and devices with smart grid features, including those at the local distribution level and those

---

264. *See supra* notes 33–37 and accompanying text. The Federal Power Act originally granted FERC jurisdiction over wholesale sales of electricity in interstate commerce and interstate electric transmission, while state PUCs reserved jurisdiction over retail electric sales, local distribution, and the siting of power plants and transmission lines. *See* Wokutch, *supra* note 40, at 545.

265. *See* Brief Amicus Curiae of Electrical Engineers, Energy Economists & Physicists in Support of Respondents in No. 00-568 at 3, New York v. Fed. Energy Regulatory Comm'n, 535 U.S. 1 (2002) (Nos. 00-568, 00-809) (explaining that while interstate electrical networks and transmissions were rare in 1935, today, "every high-voltage transmission line in the continental U.S. (outside Texas) is wired into one of the two vast interstate grids," causing the electricity transmission system to grow "away from the state regulatory territory defined by the FPA and grow[] into federal territory").

266. *New York*, 535 U.S. at 7.

267. *See supra* Part I.A.2 (discussing the compact between utilities and states that grant states substantial regulatory control over utilities in exchange for permitting utilities regional monopolies).

used directly by retail customers."[268] As one scholar notes, PUCs viewed these assertions as "throwing down the jurisdictional gauntlet" and an "unwarranted interference" with their authority to implement standards for distribution-level projects.[269]

However, cybersecurity is a trait uniquely integral to this new Smart Grid, with little history in the Traditional Grid.[270] It is a twenty-first century concern that has national security and privacy implications linked to new technologies. NIST found that most states had "little or no documentation available" for review by the Cyber Security Working Group's Privacy Subgroup.[271] Even some PUCs, despite their general opposition to federal intervention, have recognized that cybersecurity may be a special area over which federal regulatory authority is appropriate.[272]

In light of the highly interconnected, interstate nature of the electricity industry that has been acknowledged by the Supreme Court in *New York v. FERC*, congressional legislation granting top-to-bottom federal regulatory authority over the narrow area of Smart Grid cybersecurity is likely justified under the Constitution's Commerce Clause.[273] The Supreme Court has held that where there is a clear interstate market that is within the federal government's authority to regulate and can be substantially affected by intrastate commercial activity, the intrastate activity can be federally regulated under the Commerce Clause.[274] Smart Grid businesses are engaged in

---

268. Smart Grid Policy, 74 Fed. Reg. 37,098, 37,101 (July 27, 2009). FERC explains that it so interprets its jurisdiction because "Congress [did] not exclude from the scope of EISA 1305(d) facilities used in local distribution, or otherwise limit [FERC] authority to approve standards." *Id.*

269. *See* Eisen, *supra* note 172, at 56 n.237; *see also* Radford, *supra* note 257.

270. Historically, electric meter readings were taken in person, showed lump-sum longer-term energy usage (as opposed to appliance-specific usage in the Smart Grid), and were not shared in ways anticipated in the Smart Grid. Therefore, energy consumption patterns were not a matter that rose to public concern. *See* NIST GUIDELINES VOL. 2, *supra* note 42, at 9.

271. *See id.*

272. *See* Eisen, *supra* note 172, at 55 n.344 (discussing Michigan Public Service Commission's opposition to enforceable federal standards, except in limited areas, such as cybersecurity).

273. U.S. CONST. art. I, § 8, cl. 3.

274. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 17–18 (2005) (holding that the "purely intrastate" activity of growing marijuana for personal use could be federally regulated since Congress rationally concluded that failure to so regulate would undercut the regulation of an interstate market); United States v. Lopez, 514 U.S. 549, 560–61 (1995) (holding that the regulated intrastate activity must be an economic activity that substantially affects interstate commerce); Wickard v. Filburn, 317 U.S. 111, 124 (1942) (holding that the intrastate activity of growing wheat for personal consumption may be federally regulated since Congress could have properly

commercial activity and their cybersecurity choices could clearly have an impact on the stability of interstate power grids, the national economy, and national security—impacts that could all substantially affect interstate commerce.[275]

FERC conveyed its understanding that, under EISA, Congress gave FERC this type of comprehensive regulatory jurisdiction that did not end at the traditional border between interstate transmission and local distribution.[276] Congress should grant NIST similar authority to regulate cybersecurity amongst all Smart Grid participants, which has the support of both law and logic, as NIST is the agency with the expertise and experience to properly address these cybersecurity issues.

2. Proposed Legislative Action: NIST Should Be Granted the Authority to Issue Mandatory Enforceable Interoperability Standards

NIST has developed the expertise and experience necessary to issue uniform, mandatory, enforceable federal interoperability standards for Smart Grid participants through its development of Smart Grid work product under EISA and its regulation of federal information systems under the Federal Information Security Management Act of 2002 (FISMA).[277] NIST should be given, by statute, the responsibility and authority to issue mandatory interoperability standards for all Smart Grid participants. Despite the failure of legislation aimed at enhancing Smart Grid cybersecurity primarily by expanding FERC's authority to unilaterally institute mandatory reliability standards under FPA, the prevalence of cybersecurity legislation in both Houses indicates that the seriousness

---

considered that such activity could have a substantial effect on its effort to regulate an interstate market).

275. *See supra* notes 247–54 and accompanying text for a discussion of these impacts.

276. Congress authorized FERC to institute rulemaking proceedings to adopt standards and protocols "in interstate transmission of electric power, *and regional and wholesale electricity markets*." 42 U.S.C. § 17385(d) (2012) (emphasis added). It seems clear from the language of the statute that Congress granted federal jurisdictional authority beyond the traditional interstate transmission line. FERC so interpreted this language, finding its EISA authority applicable to "all electric power facilities and devices with smart grid features, including those at the local distribution level and those used directly by retail customers." Smart Grid Policy, 74 Fed. Reg. 37,098, 37,101 (July 27, 2009).

277. Federal Information Security Management Act of 2002, Pub. L. 107-347, 116 Stat. 2899 (portions most relevant to this note codified as amended in sections of 40 & 44 U.S.C.).

of this issue is entering the forefront of congressional consciousness.[278] A bill that focuses on interoperability standards, places sufficient authority in the hands of the appropriate agency with substantial experience to draw upon immediately, and emphasizes how all stakeholders would ultimately benefit from a uniform federal standard[279] might garner sufficient support in both Houses unlike other legislation, like the GRID Act.[280]

The substantial expertise and competence that NIST has developed and demonstrated while performing its duty under EISA has certainly been noticed. Pike Research, a global clean technology market research and consulting firm, noted in a 2011 report that a "number of well-written guidelines include the three-volume U.S. NIST Interagency Report . . . which covers smart grid cyber security strategy, architecture, high-level requirements, and data privacy."[281] However, the report notes that "[n]one of those guidelines is an enforceable standard," and that "[t]his lack of enforceable requirements leads to a scene of mass chaos in utility cyber security."[282] Many utilities, the report posits, "will only invest in cyber security when financial punishment for not investing is threatened."[283]

Pursuant to EISA, NIST has made great progress in identifying the fundamental building blocks of Smart Grid communication systems and how they might be secured.[284] NIST's "Logical Reference Model" (LRM)[285] is a "composite high-level view of the actors within each of the Smart Grid domains."[286] The model identifies key actors in each domain, providing a title and description for each,[287] as well as the unique communication paths between those actors, referred to as

---

278. *See supra* Part III.C.

279. *See supra* Part V.A.3.

280. *See supra* Part III.C.

281. *See* PIKE RESEARCH, *supra* note 76, at 5.

282. *Id.*; *see also* DOLEZILEK & HUSSEY, *supra* note 148, at 5 (noting that "NIST does not have authority to require compliance with NISTIR 7628, and indeed, the document was not written to facilitate compliance enforcement").

283. *See* PIKE RESEARCH, *supra* note 76, at 5.

284. *See* NIST FRAMEWORK RELEASE 1.0, *supra* note 54, at 8. NIST emphasized the need for a "common understanding of [the Smart Grid's] major building blocks and how they interrelate." *Id.* To enable this understanding, NIST developed a "conceptual architectural reference model" as a means to "analyze use cases, identify interfaces for which interoperability standards are needed, and to facilitate development of a cyber security strategy." *Id.*

285. *See* NIST GUIDELINES VOL. 1, *supra* note 38, at 17.

286. Actors are devices, computer systems, software programs, or the individuals or organizations that participate in the Smart Grid. They are needed to transmit, store, edit, and process information in the Smart Grid. *See id.* at 14.

287. *See id.* at 18–24.

"logical interfaces."[288] Each logical interface is categorized based on the Smart Grid communication process of which it is a part.[289] Graphical depictions of each category show actors involved in that category and the discrete logical interfaces between them. These visual depictions are accompanied by a legend that indicates important security considerations relevant to the particular category.[290] Having identified and analyzed these fundamental communication building blocks, NIST can regulate from a position of substantive knowledge in setting security requirements for Smart Grid communications with a focus on these fundamental blocks, allowing for a regulatory system that is applicable to diverse business models.

In determining how to convey its requirements and guide regulated entities, NIST could draw on its experience regulating federal information systems under FISMA. NIST has developed an approach under FISMA by which two primary types of publications instruct regulated entities: (1) Federal Information Processing Standard (FIPS) publications,[291] and (2) Special Publications (SPs). Although there are many FIPS publications and SPs, three are vital to the regulatory framework: (1) FIPS PUB 199 sets forth mandatory standards for categorizing information and information systems,[292] (2) FIPS PUB 200 establishes mandatory minimum information security requirements for information and information systems in each category,[293] and (3) SP 800-53 recommends ways to achieve

---

288. The logical interfaces are uniquely identified using the format UXX, where U standards for universal and XX is replaced by the specific interface number. *See id.* at 14, 17.

289. For example, the LRM identifies eleven logical interfaces that fall into "Interface Category 1" which covers interfaces "between control systems and equipment with high availability, and with compute and/or bandwidth constraints," such as communications between transmission SCADA and substation equipment, distribution SCADA and substation and pole-top equipment, or SCADA and the power plant. *See id.* at 27–29.

290. For example, several important security considerations for Interface Category 1 include "User Identification and Authentication," "Denial-of-Service Protection," and "Communication Confidentiality." *See id.* at 33.

291. FIPS publications are approved by the Secretary of Commerce and must be complied with for federal information systems under the Federal Information Security Management Act of 2002. *See* 40 U.S.C. § 11331(b)(1)(B)–(C) (2012).

292. COMPUTER SEC. DIV., NAT'L INST. OF STANDARDS & TECH., FIPS PUB 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (2004), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

293. COMPUTER SEC. DIV., NAT'L INST. OF STANDARDS & TECH., FIPS PUB 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION

compliance.[294] NIST could draw upon these publications and experiences in establishing mandatory minimum cybersecurity standards[295] and providing useful guidance to the Smart Grid industry.[296]

In addition to granting NIST the authority to develop and issue these standards, several considerations are important for potential legislation. An enforcement authority provision would be necessary to reinforce the mandatory nature of the standards. Other elements that should also be considered for incorporation into proposed legislation include the involvement of industry members, compliance certification and possible "safe harbor" implications, and the ability of the mandatory standards to evolve.

Potential legislation should grant a suitable entity enforcement authority; perhaps similar to the authority granted the ERO for the enforcement of reliability standards promulgated under the EPAct.[297] The Federal Trade Commission (FTC) might be an appropriate enforcement entity in light of its recent enforcement proceedings aimed at holding companies responsible for cybersecurity vulnerabilities in their systems as constituting "unfair and deceptive practices."[298] Some have displayed concern over the FTC's "willingness to dictate cybersecurity standards absent any regulatory or legislative guidance regarding the scope, nature, or technical details of those standards."[299] As it pertains to the Smart Grid, mandatory enforceable standards developed by NIST would fill this legislative/regulatory void, allowing NIST the ability to focus on one of its core competencies—standards development—while the FTC exercises its enforcement expertise in reliance upon the NIST standards.

SYSTEMS (2006), *available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

294. NAT'L INST. OF STANDARDS & TECH., *supra* note 263.

295. FIPS 200 can serve as an effective resource in determining minimum requirements. *See* COMPUTER SEC. DIV., *supra* note 293.

296. SP 800-53 would be an effective model from which to draw on for this purpose. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 263.

297. *See* 16 U.S.C. § 824o(e) (2012).

298. *See, e.g.*, Jorge L. Contreras et. al., *Mapping Today's Cybersecurity Landscape*, 62 AM. U. L. REV. 1113, 1125 (2013) (discussing an enforcement proceeding initiated by the FTC against HTC America); Jonathan T. Rubens, *So Many Privacy Rules! The Developing Standard of Care for Data Security and Identity Theft Protection*, BUS. L. TODAY (Jul./Aug. 2009), http://www.search.abanet.org/buslaw/blt/2009-07-08/rubens.shtml.

299. Contreras, *supra* note 298.

Industry can, and perhaps should, be involved in the standards development process. In the reliability sphere, FERC relies upon NERC, an organization representing a broad array of Smart Grid stakeholders,[300] to develop mandatory standards. In the interoperability sphere, legislation could either allow or require NIST to incorporate contributions by a representative group (perhaps SGIP[301]) in developing its mandatory standards to ensure that stakeholders are active participants in the process without unduly slowing it down.[302] The potential legislation could then grant NIST the responsibility of submitting the interoperability standards for public comment and promulgation by the Director of the Office of Management and Budget, in consultation with the Secretary of Homeland Security, similar to the promulgation procedure established under FISMA.[303]

NIST has recently completed "Phase 3" (the final phase) of its "Plan for Interoperability Standards," which entailed developing a framework for testing and certification of how standards are implemented in Smart Grid devices, systems, and processes.[304] A certification system would support the integration of the mandatory standards proposed in this Note, possibly giving rise to a statutory "safe harbor" from certain liability for certified compliant businesses, similar to that which is utilized in state regulation of the payment card industry.[305]

---

300. *See supra* note 158 and accompanying text (discussing the representative aspects of NERC).

301. *See supra* note 173 and accompanying text (discussing the representative aspects of SGIP).

302. One critique of the NERC-led process under the EPAct that gave rise to the proposal of the GRID Act in the House of Representatives was NERC's perceived failure to take prompt action on grid security vulnerabilities. *See* MARKEY REPORT, *supra* note 87, at 8 (noting, for example, that "more than six years after the identification of the Aurora vulnerability . . . NERC still has not proposed any reliability standard directly addressing that vulnerability").

303. *See* 40 U.S.C. § 11331(b)(1) (2012).

304. NIST indicated that it has now completed its three-phase plan to establish interoperability standards and protocols in a preliminary draft of its third release of its "NIST Framework and Roadmap for Smart Grid Interoperability Standards" document, the final version of which is planned for publication in the first half of 2014. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 3.0 (DRAFT) 11 (2014), *available at* http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

305. Similar "safe harbor" provisions have been instituted by state legislatures that have chosen to mandate PCI-DSS compliance by statute. In Washington, a law was passed holding some entities liable for certain damages if their negligence proximately caused the damages caused by unauthorized access to account

Any proposed or potential legislation should also recognize that interoperability standards need to be capable of evolving over time to address new challenges that arise.[306] There should be allowance for incremental alterations to regulatory catalogs of standards so that the standards can grow with technologies, rather than "preserve technologies in amber, making them potentially obsolete later."[307]

CONCLUSION

The Smart Grid offers a number of benefits in the areas of environmental consciousness, energy reliability and cost savings, and new business opportunities. Despite these benefits, the transition from an outdated Traditional Grid to an Internet-wired Smart Grid presents a number of serious national security and privacy risks. While regulatory standards issued to protect Smart Grid reliability are mandatory, standards aimed at ensuring secure interoperability are not similarly mandated. The stakes are too high to justify the current environment in which adoption of important cybersecurity standards remain merely voluntary. The rapid rate at which the Smart Grid is developing demands immediate action to ensure its resistance to cyber attacks. Legislation authorizing a federal agency to develop and issue mandatory enforceable interoperability standards would allow for a uniform, coherent approach aimed at consistent protection of information travelling throughout the complex Smart Grid network. NIST, given its demonstrated expertise in the Smart Grid arena and its experience issuing mandatory standards for federal information systems under FISMA, is the appropriate entity to be given the authority and responsibility to develop and issue these crucial standards. Such legislative action would help to safeguard the security of the United States and the privacy of its citizens by holding participants in this industry accountable for their dedication to cybersecurity, while also providing

---

information under the entity's control. *See* WASH. REV. CODE ANN. § 19.255.020(3)(a)–(b) (West 2010). However, the statute provides for a "safe harbor" by which entities would not be liable if they were "certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach." § 19.255.020(2)(b).

306. This benefit of adaptability is recognized in SP 800-53, which aimed to provide a "stable, yet flexible catalog of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements, and technologies." NAT'L INST. OF STANDARDS & TECH., *supra* note 263, at 2.

307. Eisen, *supra* note 172, at 51–52 (discussing this concern of utilities, PUCs, and others that commenters raised in their opposition to the idea of FERC setting mandatory interoperability standards under EISA).

them with the sense of regulatory stability necessary for an unwavering commitment to future innovation.