American University National Security Law Brief

Volume 8 | Issue 1 Article 2

2018

How Cybersecurity Regulation for the Smart Grid Could Upset the Current Balance of Federal and State Jurisdiction in Electricity Regulation

Cynthia Anderson
American University Washington College of Law

How Cybersecurity Regulation for the Smart Grid Could Upset the Current Balance of Federal and State Jurisdiction in Electricity Regulation

Cynthia Anderson*

I. INTRODUCTION

It is a truism to say that electricity is integral to modern life, from the basic uses of providing light and heating to the more modern economic necessity of the Internet. A widespread or long-term electric grid failure would devastate the United States.[1] Despite continually growing reliance, significant efforts to upgrade the grid and take advantage of new technologies with the potential to transform grid efficiency and reliability have only been underway for about the last decade.[2] In the United States, there is a coordinated effort between the

* **Cynthia Anderson** is currently a judicial law clerk and will soon transition to an attorney-advisor role in the United States government. She holds a JD, *magna cum laude*, from American University Washington College of Law (2016) and a BA in business administration from Oregon State University (2009).

[1] Robert Miller, *Hurricane Katrina: Communications & Infrastructure Impacts*, *in* THREATS AT OUR THRESHOLD: HOMELAND DEFENSE AND HOMELAND SECURITY IN THE NEW CENTURY 191, 191 (Bert B. Tussing ed., 2006), http://cisac.fsi.stanford.edu/sites/default/files/071022_ThreatsAtOurThreshold.pdf (describing the collapse of critical infrastructure, including the electrical grid, as "catastrophic").

[2] The main legislation directing resources towards the Smart Grid was enacted in December 2007. *See* Energy Independence and Security Act of 2007, Pub. L. No. 110-140

American University National Security Law Brief, vol. 8, no. 1 (Spring 2018), pp. 43–57.

federal and state governments and the private sector to implement these technologies, creating what is referred to as the Smart Grid.[3]

Despite a general agreement between the government, private industry, and academics to pursue the Smart Grid's implementation, basic arguments about how the technologies should be implemented, and whether the U.S. regulatory environment should be restructured, as a result, are still largely unresolved.[4] Under the current framework, each state retains regulatory authority over most aspects of electricity generation and all aspects of distribution, leaving a fairly limited role for the federal government.[5] Inherent in the design of the Smart Grid, however, is an increased interconnectedness that makes differing regulatory standards all the more likely to have a significant impact on broader grid reliability and interstate commerce.[6] This potential for grid-wide impact is nowhere more clear-cut than in relation to cybersecurity standards.[7]

(2007). The organization at "the forefront of research into the feasibility of the smart grid on a large scale" was established in 2008. EarthTalk, *How Upgrading the Power Grid Will Save Energy and Money*, SCIENTIFIC AMERICAN (Apr. 6, 2009), https://www.scientificamerican.com/article/upgrading-power-grid/# (discussing the Future Renewable Electric Energy Delivery and Management Systems Center and its work with "universities, industry and national laboratories" to develop smart technologies).

[3] *See* Joel B. Eisen, *Smart Regulation and Federalism for the Smart Grid*, 37 HARV. ENVTL. L. REV. 1, 6 (2013) (indicating that both federal and state governments have begun to build "[c]omprehensive policy frameworks").

[4] *See* discussion *infra* Part III (explaining competing views over regulatory structure of the Smart Grid).

[5] *See* discussion *infra* Section II.B (discussing traditional jurisdictional lines related to electricity regulation).

[6] *See* discussion *infra* Section II.C.ii.a (detailing concerns about the potential impact of the Smart Grid structure on the security of the electric grid).

[7] As this article went to press, information was released by the United States Computer Emergency Readiness Team ("US-CERT") that underscored the potential for a cybersecurity breach of the U.S. electric grid, and the need to ensure even the most remote portions of the grid are made secure. US-CERT revealed in an Alert released March 15, 2018, that the Russian Government had "targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. *See* Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, TA18-074A (Mar. 15, 2018), https://www.us-cert.gov/ncas/alerts/TA18-074A. Although the information was

State governments and many local utilities argue that implementing the Smart Grid should not have any effect on the jurisdictional balance between the states and the federal government.[8] While this is largely accepted in relation to rate-setting and utility-siting, many academics argue that federal jurisdiction should be expanded when setting cybersecurity standards to protect against potential vulnerabilities caused by differing standards.[9]

II. BACKGROUND

A. Overview of the Electrical Grid Structure

In the United States, the electrical grid is separated into two regional interconnections and three intrastate grids.[10] The Eastern Interconnection is comprised of all of the states east of the Rockies, and portions of Canada.[11] The Western Interconnection is comprised of all of the contiguous states west of the Rockies, and portions of Canada and

recently publicized, the Russian government has been targeting U.S. critical infrastructure since at least March 2016. *Id*.

[8] *See* Eisen, *supra* note 3, at 51 (saying that "[s]tates are virtually unwilling to cede any authority to [the Federal Energy Regulatory Commission]" when it comes to regulating the Smart Grid).

[9] *See* discussion *infra* Section II.B (citing academic articles arguing that federal regulation is necessary).

[10] *See Learn More About Interconnections*, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, http://energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0 (last visited Apr. 10, 2018) [hereinafter *Learn More*] (describing the Eastern and Western Interconnections and recognizing Alaska and most of Texas as having discrete grids); William Pentland, *What is at Stake for Hawaii in NextEra Energy – HECO Merger*, FORBES (Jan. 30, 2015), http://www.forbes.com/sites/williampentland/2015/01/30/what-is-at-stake-for-hawaii-in-nextera-energy-heco-merger/ (recognizing that Hawaii, Alaska, and Texas are run separate from the regional grids due, in the case of the former two, to physical isolation).

[11] *See Learn More*, *supra* note 9 (recognizing that most of Texas is excluded from the Eastern Interconnection).

Mexico.[12] Because the regional interconnections involve the interstate transmission of electricity, federal jurisdiction to regulate is implicated in certain parts of the process, as described below.[13]

There are three distinct components to the electrical grid for regulatory purposes—generation, transmission, and distribution.[14] Electricity generation occurs at individual, intrastate plants utilizing a variety of methods, including coal-burning, nuclear reaction, and solar conversion.[15] Generated electricity is routed through high-power, intrastate voltage lines for transmission to meet usage needs across the entire interconnection.[16] While bulk electricity sales do occur directly among providers along the high-voltage transmission lines, final distribution to end consumers such as businesses and individual homes is facilitated by local utility companies.[17] Despite the integrated ability to transmit power generated in one state to an end user in another, providers have had limited visibility into issues along the grid.[18] Representative of this limited visibility is the fact that "utilit[ies] often only know[] where an outage is located when [they] receive[] a customer's phone call."[19]

---

[12] *Id.* Note, although the Eastern and Western Interconnections both extend beyond the boundaries of the United States, that does not change anything discussed below regarding jurisdictional authority.

[13] *See* discussion *infra* Section I.B (describing the existing federal and state jurisdictional boundaries). Note that because their grids are contained wholly within the borders of one state, Hawaii, Alaska, and the majority of Texas are not subject to federal jurisdiction and are thus outside of the scope of this paper. *See* Pentland, *supra* note 9.

[14] *See, e.g.*, New York v. Fed. Energy Reg. Comm'n, 535 U.S. 1, 5–6 (2002) [hereinafter *New York v. FERC*] (recognizing generation, transmission, and distribution as fundamental aspects of providing electricity and that Congress drew jurisdictional lines along those three categories in the Federal Power Act ("FPA") of 1935).

[15] Ashira Pelman Ostrow, *Grid Governance: The Role of a National Network Coordinator*, 35 CARDOZO L. REV. 1993, 2001 (2014).

[16] *See id.* (explaining that transmission networks have been increasingly interconnected to increase grid reliability and defray costs of expensive new power plants through co-ownership).

[17] *See New York v. FERC*, 535 U.S. at 10–11 (recognizing that transmission lines are integral to the bulk power market but that sales to retail customers occur through state-regulated utility companies).

[18] *See* Eisen, *supra* note 3, at 8 (noting a general failure to use sensors and other technology for monitoring).

[19] *Id.*

B. Federal and State Jurisdictional Lines in Electricity Regulation

Federal jurisdiction over the electrical grid is derived from Congress's constitutional authority to regulate interstate commerce.[20] Regulatory authority is, therefore, divided between the state and federal governments based on whether the function of an action or regulated entity is intrastate or interstate in nature. Jurisdictional boundaries have essentially followed those established by Congress under the Federal Power Act of 1935 ("FPA").[21]

The FPA provides for federal jurisdiction over the transmission and wholesale sale of electric energy in interstate commerce.[22] It specifically exempts from federal jurisdiction any facilities used in electricity generation, local distribution, and intrastate transmission.[23] Thus, of the three components of the electrical grid, only transactions associated with high-voltage interstate transmission lines fall under the *general* jurisdiction of the Federal Energy Regulatory Commission ("FERC").

Although FERC only has general authority to regulate interstate transmission and wholesale sales, it does have limited jurisdiction over electricity generation facilities. The Energy Policy Act of 2005 amended the FPA to extend federal jurisdiction over "generation facilities needed to maintain transmission system reliability" for purposes of mandatory grid reliability standards affecting interstate transmission and the bulk-power system.[24] Accordingly, the federal government has *some* form of regulatory authority over two of the three components of the electrical grid.

---

[20] *See, e.g.*, *New York v. FERC*, 535 U.S. at 5–6 (explaining that the Federal Power Act of 1935 was enacted to provide for federal regulation over aspects of the electrical grid that states could not regulate under the Commerce Clause).

[21] *See* Christopher Bosch, Note, *Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards*, 41 FORDHAM URB. L.J. 1349, 1398 (2014) (noting that the FPA provided the original statutory basis for federal regulation of the electric grid, though the scope of allowed regulation has grown over time due to increased interconnectedness of the grid).

[22] 16 U.S.C. § 824(a) (2014).

[23] *Id.* § 824(b)(1).

[24] *Id.* § 824o(a)(1)(B); *see also id.* at § 824o(b) (defining commission jurisdiction).

Though there is no explicit statutory authority for federal regulation of distribution-level public utilities, some voluntary actions by the utilities can bring them under FERC jurisdiction for rate-setting purposes. In *New York v. FERC*,[25] the Supreme Court reviewed FERC Order No. 888, which, *inter alia*, required application of a single tariff for all utilities purchasing transmission services whenever retail utilities voluntarily unbundled generation and transmission pricing.[26] New York argued that FERC had exceeded the boundaries of its jurisdiction in attempting to regulate unbundled retail transmission prices because all retail transactions were "properly the subject of state regulation."[27] The Supreme Court rejected New York's argument, however, and concluded that FERC did have jurisdiction to regulate the unbundled retail transmission of electricity because it had jurisdiction over any transmission in interstate commerce and "the nature of the national grid" results in all electricity transmission being aggregated on the same transmission lines.[28]

C. The Smart Grid

The Smart Grid is a coordinated effort across the electricity industry to create "robust communication paths between end-use consumers . . . and upstream to the utilities, or other energy service providers."[29] There are five categories of Smart Grid systems being implemented[30]:

---

[25] *New York v. FERC*, 535 U.S. 1.

[26] *Id.* at 11.

[27] *Id.* at 16.

[28] *Id.* at 17. *See id.* at 7, 17, 20 (reviewing the structure of the electrical grid and concluding that transmission was inherently interstate in nature and therefore properly subject to federal regulation, regardless of whether the end purchaser was wholesale or retail).

[29] Ray Gifford & Eric Gunning, *Telecommunications & Electronic Media: The Opportunity and Peril of Smart Grid*, 11 ENGAGE 128 (2010).

[30] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-117, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 7 tbl.1 (2011) [hereinafter "GAO Report"] (explaining the Smart Grid system categories described by the National Energy Technology Laboratory ("NETL")).

(1) Integrated communications;[31] (2) advanced components;[32] (3) advanced control methods;[33] (4) sensing and measurement;[34] and (5) improved interfaces and decision support.[35] The U.S. Department of Energy lists the following anticipated benefits of the Smart Grid technologies include:

- More efficient transmission of electricity
- Quicker restoration of electricity after power disturbances
- Reduced operations and management costs for utilities, and ultimately lower power costs for consumers
- Reduced peak demand, which will also help lower electricity rates
- Increased integration of large-scale renewable energy systems
- Better integration of customer-owner power generation systems, including renewable energy systems
- Improved security[36]

---

[31] Integrated communication systems are "[h]igh-speed, fully integrated, two-way communications technologies" that allow for "real-time information and power exchange." *Id.* These technologies are implemented along the distribution channels or in consumer homes. *Id.*

[32] Advanced component systems utilize the latest technologies to "produce higher power densities, greater reliability and power quality . . . and improved real-time diagnostics." *Id.* Examples include enhanced use of storage devices, "smart appliances" in consumer homes and businesses, and local "microgrids" that can operate independently from the larger grid when necessary. *Id.*

[33] Advanced control methods systems "monitor power system components" to "improve utilization of generation and transmission assets" by, for instance, using sensors along substation and distribution facilities to automatically identify system failures. *Id.* at 8.

[34] Sensing and measurement systems provide information about equipment functionality and consumer demand to utility companies and inform consumers about current prices and demand. *Id.* This is accomplished through use of "smart meters," sensors, "[c]onsumer portals," and "[d]ynamic line-rating devices." *Id.*

[35] Improved interface and decision support systems utilize software to analyze system data and enable utility employees to make "more accurate and timely" decisions. *Id.*

[36] OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, *What is the Smart Grid?*, SMARTGRID.GOV, https://www.smartgrid.gov/the_smart_grid/smart_grid.html (last visited Apr. 10, 2018).

i. Energy Independence and Security Act of 2007

While efforts were initiated by private industry, both federal and state legislators have taken steps to promote the initiative.[37] The primary federal statute regulating Smart Grid progress is the Energy Independence and Security Act of 2007 ("EISA").[38] EISA lays out ten goals for the Smart Grid that, together, are intended to "maintain a reliable and secure electricity infrastructure that can meet future demand growth . . . ."[39] Additionally, it provides direction for the creation of a uniform framework of interoperability standards that will ensure all components of the Smart Grid can interact effectively and securely.[40] In doing so, it provides for some additional federal jurisdiction over the electricity industry.[41]

EISA assigns the National Institute of Standards and Technology ("NIST") primary responsibility for coordinating the development of a framework of interoperability standards for the Smart Grid.[42] It requires NIST to solicit input from other federal committees, including the Smart Grid Task Force and the Smart Grid Advisory Committee,[43] as well as state agencies and private industry.[44] The NIST standards

---

[37] *See* GAO Report, *supra* note 29, at 4 (acknowledging that electricity industry made initial steps towards updating the grid to take advantage of new technologies); Eisen, *supra* note 3, at 6 (indicating that both federal and state governments have begun to build "[c]omprehensive policy frameworks").

[38] *See* Eisen, *supra* note 3, at 5 (explaining that Congress enacted EISA to prescribe the Smart Grid standards-setting process).

[39] 42 U.S.C. § 17381 (2014). EISA's ten listed goals for the Smart Grid system inform the work conducted by the NETL and the National Institute of Standards and Technology ("NIST") as described *supra* notes 21–26 and accompanying text.

[40] 42 U.S.C. § 17385(a)–(b) (2012).

[41] *See* discussion *infra* Section II.C.i (describing EISA-based federal jurisdiction).

[42] 42 U.S.C. § 17385(a).

[43] *Id.* § 17383(a)(1). The Smart Grid Task Force and Smart Grid Advisory Committee were established under EISA to act in an advisory capacity to relevant federal agency heads by being involved in federal, state, and private Smart Grid initiatives. *See* Energy Independence and Security Act of 2007, Pub. L. No. 110-140, 121 Stat. 1492 § 1303 (2007).

[44] 42 U.S.C. § 17385(a)(1)–(2).

are required to be "flexible, uniform and technology neutral."[45] However, state and industry adoption of the NIST standards is strictly voluntary.[46]

Under EISA, FERC is provided with jurisdiction to adopt NIST interoperability standards as mandatory through rulemaking proceedings where there is "sufficient consensus" regarding the standard, and it is "necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[47] FERC has interpreted the language to mean that it has authorization to conduct rulemaking proceedings affecting distribution-level facilities, if necessary.[48] However, it is generally accepted that because EISA does not provide FERC with any additional enforcement authority, the standards will only be mandatory where they fall within FERC's other grants of jurisdictional authority under the FPA, as amended.[49]

ii. Cybersecurity Concerns

a. Identified Potential Vulnerabilities

In a 2011 report, the Government Accountability Office ("GAO") identified a number of potential vulnerabilities in the Smart Grid system.[50] The vulnerabilities included a larger number of potential entry points into the electrical grid by hackers as a result of increased integration

[45] *Id.* § 17385(b).

[46] *See* Bosch, *supra* note 20, at 1380–81 (explaining that NIST standards can only become mandatory if adopted through a FERC rulemaking proceeding in compliance with EISA requirements).

[47] 42 U.S.C. § 17385(d).

[48] *See* GAO Report, *supra* note 29, at 13 n.12.

[49] *Compare* GAO Report, *supra* note 29, at 18–19 (explaining that FERC would have the ability to enforce standards, in conjunction with the North American Electric Corporation, under its grid-reliability authorities and through incentive-based programs), *with* Eisen, *supra* note 3, at 37 (noting that FERC enforcement power is limited to "its existing FPA authorities to regulate interstate transmission of electricity").

[50] These vulnerabilities are reflected in the introductory "What GAO Found" section of the GAO Report. *See* GAO Report, *supra* note 29.

of grid components and newly implemented systems; unknown vulnerabilities inherent with new system and network technologies; the ability for hackers to affect a larger area of the grid at one time through interconnecting systems; and increased incentives to hack the system for monetary gain because of the potentially large amount of customer information stored within the system.[51] It is generally acknowledged that a single attack has the potential to cause region-wide electrical grid failures that could last for days at a time.[52] Such an occurrence could have an almost unimaginable economic and human impact, especially if a cyber-attack were coordinated with a physical terrorist attack.[53] As one commentator notes, the negative consequences of a widespread power outage are exacerbated by the interdependent nature of the nation's critical infrastructure systems, such as water and transportation, with the electrical grid.[54]

b. Attacks That Have Already Occurred

The GAO vaguely references a variety of cybersecurity issues that have already occurred or been proven to be a threat, in the United States and abroad.[55] Cybersecurity experts have shown that vulnerabilities in smart meters have the potential to allow a hacker to disrupt the electricity grid,[56] and the Central Intelligence Agency ("CIA") has

---

[51] *Id.* at 9 (listing categories of risk involving physical infrastructure).

[52] *E.g.*, Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 326–27 (2013) (discussing the means by which an attack may have wide reaching regional consequences).

[53] *Cf.* Miller, *supra* note 1 (describing the collapse of critical infrastructure, including the electrical grid, as "catastrophic").

[54] *See* Michael McElfresh, *Can the Smart Grid Survive a Cyberattack?*, ENERGY POST (June 29, 2015), http://www.energypost.eu/can-smart-grid-survive-cyberattack/ (quoting a report that called the electrical grid an obvious target for those seeking to do physical, economic and psychological harm to the nation).

[55] *See* GAO Report, *supra* note 29. The summary "What GAO Found" section acknowledges that the report was not able to adequately address the risk of attacks, despite the GAO's intention to do so.

[56] *See* Eduard Kovacs, *Smart Meters Pose Security Risks to Consumers, Utilities: Researcher*, SECURITY WEEK (Jan. 4, 2017), http://www.securityweek.com/smart-meters-pose-security-risks-consumers-utilities-researcher (explaining that hackers could hijack network traffic-connecting smart appliances and the grid and take control of devices).

already reported regional overseas power disruption as a result of "malicious activities against IT systems[.]"[57] The cited materials referencing the CIA-acknowledged attacks are no longer accessible, but there are still media reports available online. Though the media reports do not include specifics, one attack apparently resulted in a multi-city power failure, while others resulted in extortion demands.[58] The Stuxnet computer worm is also cited as an example of a significant cybersecurity concern for the U.S. electrical grid, though that attack was not carried out against an electrical grid.[59]

III. ARGUMENTS FOR AND AGAINST EXTENDING FEDERAL JURISDICTION

The arguments are fairly predictable for why or why not to extend federal jurisdiction over the electrical grid for cybersecurity standard-setting purposes. State regulators want to maintain the existing jurisdictional boundaries, which would keep federal involvement limited to aspects involving interstate transmission and wholesale sales.[60] Many academics argue, however, that it is necessary for federal jurisdiction to extend over the entire electrical grid for cybersecurity standard-setting purposes, to ensure consistency and compliance.[61] Each of these arguments contains additional nuance, explored further below.

Researchers have said that the security vulnerabilities have persisted, despite initial studies showing their existence in 2010. *Id.*

[57] *See* GAO Report, *supra* note 29, at 10.

[58] Tom Espiner, *CIA: Cyberattack Caused Multiple-City Blackout*, CNET NEWS (Jan. 22, 2008), https://www.cnet.com/news/cia-cyberattack-caused-multiple-city-blackout/.

[59] *See* McElfresh, *supra* note 53 (explaining how the systems used to operate the Smart Grid are substantially similar to those that were compromised by the Stuxnet computer worm, which shut down Iranian centrifuges used for uranium enrichment); Doug Drinkwater, *Stuxnet-style Attack on US Smart Grid Could Cost Government $1 Trillion*, SC MAGAZINE (July 13, 2015), http://www.scmagazineuk.com/stuxnet-style-attack-on-us-smart-grid-could-cost-government-1-trillion/article/426108/ (discussing a report that detailed why the U.S. electrical grid could be vulnerable to a Stuxnet-style attack).

[60] *E.g.*, Gifford & Gunning, *supra* note 28, at 130.

[61] *See* Bosch, *supra* note 20, at 1391–94 (explaining that voluntary or limited standards are insufficient because of the high stakes involved if a failure does occur).

A. Arguments for Maintaining Existing Jurisdictional Boundaries

There are essentially two categories of arguments for maintaining existing jurisdictional boundaries between state and federal governments for purposes of Smart Grid cybersecurity regulation: first, that the federal government only has enforcement authority over interstate transmission, and any further standards could only be enforced by influencing the states; and second, that there are practical concerns with mandating standards at a federal level.

It is noted that, even if FERC could mandate standards for all portions of the grid and all participants, "it [is] not clear how it would enforce a mandate."[62] Some argue that FERC "can only mandate standards for interstate transmission" and that it has no "authority over generation, middle-mile and last-mile distribution, or in-home energy management."[63] This traditional breakdown should continue to be seen in the jurisdictional boundaries for physical Smart Grid investments.[64] Thus, an attempt by the federal government to change its jurisdiction over Smart Grid cybersecurity could be seen by states as "an attempt to usurp some of the state powers with respect to the prudence of grid investments, interoperability mandates, and grid management."[65] Rather, it is necessary for federal agencies to convince states to enact the standards proposed by NIST in order to avoid legal challenges to federal jurisdictional authority.[66]

There are numerous practical concerns about a change in jurisdictional boundaries relating to cybersecurity of the Smart Grid. Specifically, the concerns relate to the potential negative effects of

---

[62] Eisen, *supra* note 3, at 51.

[63] Gifford & Gunning, *supra* note 28, at 129.

[64] *See id.* at 130 (discussing the juxtaposition between federal jurisdiction asserted over all cybersecurity of the smart grid with the retained traditional jurisdictional boundaries for physical infrastructure investment approvals).

[65] *Id*.

[66] *See* Resolution, Nat'l Ass'n of Reg. Util. Commissioners, Resolution Regarding Smart Grid (July 22, 2009), https://pubs.naruc.org/pub.cfm?id=53985C5D-2354-D714-51F0-F9226449 C37D (emphasizing the need for the federal government to partner with the state regulatory authorities in creating policies and standards for the Smart Grid and emphasizing jurisdictional lines for FERC and the state governments).

mandatory regulation.[67] For instance, private-sector commentators noted that it prefers voluntary standards because they are more flexible and less likely to be set arbitrarily or to remain in place despite becoming obsolete.[68] State governments and electricity providers expressed concern that any mandatory rules, even if limited to areas of traditional jurisdiction, would "gain traction and work their way down to the local level."[69] Thus, in effect, any federal rules would become the standard across all levels and undermine state authority to regulate.[70]

B. Arguments for Extending Federal Jurisdiction to Include Cybersecurity of all Aspects of the Smart Grid

Even proponents of extending FERC's jurisdiction do not assert that its enforcement authority was affected by EISA.[71] Rather, the arguments rest on the fact that FERC and the North American Electric Reliability Corporation ("NERC") can, in fact, promulgate rules under those acts—enforcement concerns aside—and that mandatory rules are simply necessary.[72] One reason why mandatory standards across the entire grid are necessary is that a grid failure would have such devastating consequences.[73] For instance, the aggregate impact of

---

[67] *See* Eisen, *supra* note 3, at 51 (identifying mandatory regulations as one of the greatest concerns for Smart Grid commentators).

[68] *See id.* at 51–52. (expressing concerns about mandatory FERC requirements and potential monopolization of the energy sector).

[69] *Id.* at 51.

[70] *Cf.* ROGER LEVY ET AL., SMART GRID STANDARDS: IMPLICATIONS FOR STATE REGULATORY COMMISSIONS; BACKGROUND AND FREQUENTLY ASKED QUESTIONS 13 (Nov. 2010), https://emp.lbl.gov/sites/default/files/naruc-nist111010.pdf (noting the potential for federal agency adoption to create jurisdictional issues while asserting that adoption of mandatory standards by some states could impact operations in other states in the interconnection).

[71] *See* Bosch, *supra* note 20, at 1392–93 (noting that EISA was unclear about how FERC would enforce the standards it allowed FERC to promulgate via rulemaking, but that FERC did not interpret its enforcement authorities to have been modified by the statute).

[72] *See id.* at 1393 (listing industry concerns resulting from a lacking standard).

[73] *See id.* at 1394 (emphasizing electricity's significant role in daily lives); *see also supra* notes 41–47 and accompanying text.

"smart grid home device[s]" on the bulk power grid could result in wide-spread reliability or security issues across an interconnection.[74] In addition, proponents argue that, rather than being negative for the industry by risking stagnant standards, a uniform approach would benefit stakeholders by providing certainty that investments into security and infrastructure will comply with requirements and thus industry stakeholders will not "risk losing their entire investment if future laws invalidate their approach."[75]

IV. CONCLUSION

Cybersecurity of the Smart Grid presents a unique problem regarding decades-old and long-settled jurisdictional boundaries in the area of electricity regulation. Because vulnerabilities at a single point on the Smart Grid could result in power failure on an interstate or regional scale, the concept of local distribution of power does not apply as directly as it would in traditional transactions. Though Congress has passed a law that does provide FERC with authority to promulgate rules-setting standards for cybersecurity of the Smart Grid, there remains controversy over whether, and to what extent, federal jurisdiction has been or should be broadened.

Industry commentators argue that mandatory rules set by the federal government will often be behind the curve on what is technologically possible and will be left in place long after becoming obsolete. Thus, the Smart Grid would inherently have unnecessary vulnerabilities that would be addressed by using the most up-to-date knowledge and technologies. On the other hand, proponents of expanding federal jurisdiction point out that whenever standards are not mandatory, some actors will always fail to implement necessary

---

[74] North American Electric Reliability Corporation, Comment of the North American Electric Reliability Corporation in Response to the Commission's March 19, 2009 Proposed Smart Grid Policy Statement 11 (May 11, 2009), http://www.nerc.com/files/NERCSmartGridPolicy StatementComments.pdf.

[75] *See* Bosch, *supra* note 20, at 1396–97 (quoting BOB LOCKHART & BOB GOHN, PIKE RESEARCH, UTILITY CYBER SECURITY: SEVEN KEY SMART GRID SECURITY TRENDS TO WATCH IN 2012 AND BEYOND 5 (2011)) (describing how uncertainty about standards at early stages is likely preventing investment and innovation).

safeguards. Because of the interconnected nature of the Smart Grid, any single vulnerability would have far-reaching consequences. Thus, a uniform approach would benefit stakeholders by providing clear guidance that supports investment in costly infrastructure and technology upgrades.