

Barry Law Review

Volume 24

Issue 1 *Barry Law Review: Fall 2018*


Article 3

1-1-2019

The Threat Is Real: Protecting The Energy Infrastructure From Cyberattacks

Patricia Blotzer

Follow this and additional works at: <https://lawpublications.barry.edu/barryrev>

 Part of the [Administrative Law Commons](#), [Energy and Utilities Law Commons](#), [Environmental Law Commons](#), [International Law Commons](#), [Internet Law Commons](#), [Jurisprudence Commons](#), and the [Other Law Commons](#)

Recommended Citation

Patricia Blotzer (2019) "The Threat Is Real: Protecting The Energy Infrastructure From Cyberattacks," *Barry Law Review*: Vol. 24 : Iss. 1 , Article 3.

Available at: <https://lawpublications.barry.edu/barryrev/vol24/iss1/3>

This Article is brought to you for free and open access by Digital Commons @ Barry Law. It has been accepted for inclusion in Barry Law Review by an authorized editor of Digital Commons @ Barry Law.

THE THREAT IS REAL: PROTECTING THE ENERGY INFRASTRUCTURE FROM CYBERATTACKS

Patricia Blotzer*

INTRODUCTION

After the recent suspected hacking incidents including the Sony hack by North Korea in 2014, and more recently the 2016 Election hacks by Russia, both legislators and citizens are taking the threat and possibility of cyber threats to our nation's energy infrastructures more seriously than ever. For many Americans, the realization that our nation's election system may have been hacked is not only scary, but makes the possibility of hacking and cyber terrorism seem more possible than ever before.

On November 24, 2014, Sony experienced a cyberattack that brought the company to its knees.¹ As employees turned on their computers, they found the computers had been infected with malware displaying threats and “the menacing image of a fiery skeleton looming over the tiny zombified heads of the studio's top two executives” on their screens.² The malware spread from computer to computer throughout the company and across continents, erasing everything on 3,262 of 6,797 computers Sony owned, and deleting everything from 837 of 1,555 Sony servers.³ After erasing the data from the computers, the malware then deleted the startup software, making the computers useless.⁴ Then the hackers released the data they had stolen, including movie scripts, unreleased films, confidential emails, and over 47,000 social security numbers.⁵ It was speculated the hack was done to prevent Sony from releasing the movie *The Interview*.⁶ The cyberattack on Sony helped open America's eyes to the fact that cyber threats are real, and can happen to anyone, including big corporations.

* Barry University School of Law, Juris Doctor, May 2018; Webster University, Master of Health Administration, October 2011; University of Central Florida, B.A. Advertising/Public Relations, May 2003. First and foremost, I would like to express my deepest gratitude to Professor Nadia Ahmad, without her guidance this article would not be possible. I would also like to thank Professor Wes Henriksen, for his constant advice and support on my journey to being published.

1. Peter Elkind, *Sony Pictures: Inside the Hack of the Century, Part 1*, FORTUNE (June 25, 2015, 6:00 AM), http://fortune.com/sony-hack-part-1/?xid=for_em_sh, archived at <https://perma.cc/E9XA-MJX7> [hereinafter Elkind, *Sony, Part 1*].

2. *Id.* Some experts remain unconvinced North Korea was behind the Sony cyberattacks. One reason is because it is easy and normal for hackers to leave false clues behind. The FBI concluded North Korea was behind the hacks after only 25 days, which many feel is too short a time to have fully conducted an investigation, and the FBI refuses to make the evidence that North Korea was responsible available to the public. See Peter Elkind, *Sony Pictures: Inside the Hack of the Century, Part 3*, FORTUNE (June 27, 2015, 8:00 AM), <http://fortune.com/sony-hack-final-part/>, archived at <https://perma.cc/D7DL-CWLY> [hereinafter Elkind, *Sony, Part 3*].

3. Elkind, *Sony, Part 1, supra* note 1.

4. *Id.*

5. *Id.*

6. Elkind, *Sony, Part 3, supra* note 2. *The Interview* is a comedy where “Dave Skylark and his producer Aaron Rapoport run the celebrity tabloid show ‘Skylark Tonight’. When they land an interview with a surprise fan, North Korean dictator Kim Jong-un, they are recruited by the CIA to assassinate him.” *The Interview*, IMDB, http://www.imdb.com/title/tt2788710/?ref_=ttpl_pl_tt, archived at <https://perma.cc/7YG2-9VSM>. (last visited Aug. 16, 2018).

After America's eyes were opened by the Sony attacks, the 2016 Election hacks brought the threat of cyberattacks back to the forefront of people's minds. In the declassified report from the Office of the Director of National Intelligence, Russia was accused of hacking both Democratic and Republican targets, and using this information to "disrupt the American electoral process."⁷ The report states, "Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments."⁸ The possibility of another country having the capability to hack the election system has brought the topic of cyber security to the table for all industries, including energy, across the nation.

Most people do not realize that hacking happens every day, and there have already been hacks to the energy infrastructures of the United States (U.S.) and other countries.⁹ While some hacks are done maliciously to cause harm, such as blackouts, other hacks are actually planned, and done to test the infrastructures and to locate potential weak points.¹⁰

Cyberattacks are not only real, but they are already happening around the world. Part I of this note discusses cyberattacks that have occurred in the U.S. and other countries. Part II examines current legislation in the U.S. related to protecting the energy infrastructure from cyberattacks. Part III discusses the potential threats to, and examples of how each of four energy industries has been hacked. The four industries this note covers are: nuclear, hydro, solar, and wind.

Part IV will review current and past proposed legislation in the U.S., and will discuss if these laws adequately protect our nation's energy infrastructure from cyberattacks. In Part V, this note will consider how the energy industries and individual power companies can take action on their own to protect themselves from cyberattacks. One way they can do this is by testing their own security systems, or hiring outside companies to hack into their systems to find weaknesses. The purpose of this note is to not only educate readers about the constant threat of cyberattacks on our nation's energy infrastructures, but that there are things that can be done now to protect against cyberattacks, and that our legislators can help play a key role in protecting us going forward.

7. Andy Greenberg, *Feds' Damning Report on Russian Election Hack Won't Convince Skeptics*, WIRED (Jan. 6, 2017, 5:25 PM), <https://www.wired.com/2017/01/feds-damning-report-russian-election-hack-wont-convince-skeptics/>, archived at <https://perma.cc/2EQL-H74K>. See also AJ Vicens, *Russian Hackers May Now Be Mucking With European Elections*, MOTHER JONES (Feb. 27, 2017, 11:00 AM), <http://www.motherjones.com/politics/2017/02/what-russia-european-elections>, archived at <https://perma.cc/PLX7-G58E> (after U.S. officials warned Russia may target other countries' election systems, recent statements from Russia have led officials to believe Russia is now targeting France and Germany).

8. Greenberg, *supra* note 7.

9. Brian Naylor, *Russia Hacked U.S. Power Grid – So What Will The Trump Administration Do About It?*, NPR (Mar. 23, 2018, 5:00 AM), <https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it>, archived at <https://perma.cc/8M4V-D72X>.

10. Andy Greenberg, *Hackers Gain Direct Access to US Power Grid Controls*, WIRED (Sep. 06, 2017, 6:00AM), <https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/>, archived at <https://perma.cc/68LH-33JT>.

I. CYBERATTACKS TO ENERGY INFRASTRUCTURES ARE ALREADY HAPPENING

A. Ukrainian Energy Hacks

Ukraine fell victim to one of the first known cyberattacks on a civilian population resulting in power outages in 2015.¹¹ On December 23, one of Ukraine's power distributors had 27 substations suddenly go dead, leaving 103 cities in the dark, and another 186 cities in partial darkness.¹² Teams had to be sent around the region to manually flip the switches back on,¹³ restoring the power after six hours.¹⁴

The cyberattack on Ukraine's power grid started months earlier, when the energy company's computers were infected with malware.¹⁵ It is believed someone at the company received and opened an infected Microsoft Word document, allowing the malware into the computer systems.¹⁶ When the power went out, the call centers for the power companies suddenly received thousands of calls from a remote adversary, with the purpose of "deny[ing] access to . . . customers calling in and reporting the outage."¹⁷

Almost a year later, on December 17, 2016, Ukraine's power grid was hacked again.¹⁸ The second attack occurred around midnight and lasted only an hour.¹⁹ Ukrainian officials believe the second attack was done by the same hackers who did the first.²⁰ The second attack could have done more damage, but the hackers only seemed to want to make "a demonstration of [their] capabilities."²¹ The second attack is believed to have begun in July during an immense phishing campaign that targeted many government offices, and once the hackers gained access, they watched and waited before making their presence known.²²

When a cyberattack is not discovered early on, the hacker can watch the system undetected for months.²³ Once inside, hackers will often steal administrator credentials, and conduct reconnaissance, watching network traffic and studying daily behaviors.²⁴ "Ukraine 'has turned into a training playground for research and development of novel attack techniques'—attacks that will likely be used elsewhere once the hackers refine them."²⁵ One concern for the U.S. is, because our energy grid is

11. Kim Zetter, *The Ukrainian Power Grid Was Hacked Again*, MOTHERBOARD (Jan. 10, 2017, 10:07 AM), https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report, archived at <https://perma.cc/C8NY-W26X>.

12. Jose Pagliery, *Scary Questions in Ukraine Energy Grid Hack*, CNN TECH (Jan. 18, 2016, 2:37 PM), <http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/>, archived at <https://perma.cc/975L-VD3X> [hereinafter Pagliery, *Scary Questions*].

13. *Id.*

14. Zetter, *supra* note 11.

15. Pagliery, *Scary Questions*, *supra* note 12.

16. *Id.*

17. *Id.*

18. Zetter, *supra* note 11.

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.* For an explanation of phishing, see *infra* Part V C.

23. Zetter, *supra* note 11.

24. *Id.*

25. *Id.*

more automated than in Ukraine, if we were to fall victim “to the same kind of attack as the one in Ukraine, manually flipping switches back ‘on’ won’t be as easy.”²⁶

B. Canadian Energy Hacks

In November 2016, Canada’s federal intelligence agency, the Communication Security Establishment (CSE), released statistics of known “system compromises.”²⁷ The information released showed Canada’s natural-resources, energy, and environment sector was targeted by hackers almost as much as all other sectors combined.²⁸ This sector was targeted 2,078 times in 2016,²⁹ whereas hacking attempts to all other sectors combined totaled 2,493.³⁰ The Canadian government also reported that of the 4,571 known compromises, information was stolen in only three instances, and in all three the information was not classified.³¹ One of these three instances was from the natural-resources, energy, and environment sector.³²

The CSE did not give specifics as to which specific departments were targeted by hackers, nor did they state the origin of the attacks.³³ A CSE spokesman stated that “CSE will not provide details about ‘specific cyber threat actors or cyber security incidents,’ in order to protect the efficiency of classified cyber-defense methods that secure the government’s networks.”³⁴ The CSE does block over 100 million attempted hacks every day.³⁵

In December 2016, the U.S. Department of Homeland Security (DHS) warned Canada that an IP address at an Ontario electricity distributor, Hydro One, may have been the target of a Russian cyberattack.³⁶ The U.S. government discovered the possible attack while investigating the 2016 Election hacks.³⁷ This possible cyberattack involved Russian malware that may have been downloaded into computers at Hydro One.³⁸ The company has stated that “they take cyber security seriously” and that “the address in question is not an active IP address at Hydro One, nor is it connected to the power system,” indicating the Canadian energy grid was not at risk.³⁹

26. Pagliery, *Scary Questions*, *supra* note 12.

27. Colin Freeze, *Hackers Target Canadian Government’s Energy and Resource Departments*, GLOBE & MAIL (Nov. 17, 2016, 2:15 PM), <http://www.theglobeandmail.com/news/politics/hackers-target-governments-energy-and-resource-departments/article32890960/>, archived at <https://perma.cc/9Z7L-RF6Y>. See generally COMMUNICATIONS SECURITY ESTABLISHMENT, <https://www.cse-cst.gc.ca/en/inside-interieur/protect-protection>, archived at <https://perma.cc/PNY6-ETDR> (last visited Nov. 22, 2018) (the goal of Canada’s CSE is to safeguard and protect Canada’s computer networks with leading-edge technology).

28. Freeze, *supra* note 27.

29. *Id.*

30. *Id.*

31. Andrew Silver, *Why Do Hackers Love to Attack Canada’s Energy Departments?*, IEEE SPECTRUM (Dec. 2, 2016, 2:30 PM), <http://spectrum.ieee.org/energywise/energy/the-smarter-grid/why-do-hackers-love-to-attack-canadas-energy-environment-and-natural-resources-sector>, archived at <https://perma.cc/T32F-XMFS>.

32. *Id.*

33. Freeze, *supra* note 27.

34. Silver, *supra* note 31.

35. *Id.*

36. *Exclusive: IP Address at Ontario Power Utility Linked to Alleged Russian Hacking*, CTVNEWS (Jan. 3, 2017, 6:28 PM), <http://www.ctvnews.ca/canada/exclusive-ip-address-at-ontario-power-utility-linked-to-alleged-russian-hacking-1.3226290>, archived at <https://perma.cc/RVK4-ZK39> [hereinafter *Exclusive*].

37. *Id.*

38. *Exclusive*, *supra* note 36.

39. *Id.*

C. U.S. Energy Hacks

The U.S., like Canada, is somewhat silent on details involving hacks to the nation's energy infrastructures. In 2014, the energy grid was attacked 79 times, but the government would not provide specific information, simply stating the "incidents involved attacker techniques."⁴⁰ Vermont's Burlington Electric recently found malware on a company owned laptop.⁴¹ Following the recommended procedures set out by the North American Electric Reliability Corporation (NERC), the company notified federal officials as soon as the malware was discovered, and an investigation on how the malware got on the laptop was initiated.⁴² The Vermont hack was described as "an example of the system working."⁴³ The electric company said the laptop was not connected to the grid, and officials are not sure if the intent of the cyberattack was to interrupt operations or to just test the system to determine if it was penetrable.⁴⁴

In the past, China, Russia, and other countries have been suspected of attempting to hack into the nation's utility companies.⁴⁵ DHS released a report stating they believe Advanced Persistent Threat (APT) nations are targeting the U.S. primarily for conducting cyber espionage.⁴⁶ APT actors successfully infiltrated the energy sector 17 times during 2014, but did not cause any damage or disruptions to service.⁴⁷ DHS reported, "the majority of malicious activity occurring against the energy sector is low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector, is financially or ideologically motivated, and is not meant to be destructive."⁴⁸

While the report plays down the severity of these known hacks to our energy infrastructures, critics feel these cyberattacks should not be taken lightly.⁴⁹ In one of the 17 known cyber hacks, the hackers are suspected of stealing data from a petroleum organization.⁵⁰ DHS downplays the seriousness of these cyberattacks, claiming the hackers are only hacking into the energy systems to facilitate a disruption of

40. Jose Pagliery, *Government reveals details about energy grid hacks*, CNN TECH (Apr. 5, 2016, 3:37 PM), <http://money.cnn.com/2016/04/05/technology/energy-grid-hacks/>, archived at <https://perma.cc/P965-2YYH> [hereinafter Pagliery, *Government reveals*].

41. Juliet Eilperin & Adam Entous, *Russian operation hacked a Vermont utility; showing risk to U.S. electrical grid security, officials say*, WASH. POST (Dec. 31, 2016), https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.943e817cb123, archived at <https://perma.cc/47Z8-YC2K>.

42. Ellen Nakashimi & Juliette Eilperin, *Russian government hackers do not appear to have targeted Vermont utility, say people close to investigation*, WASH. POST (Jan. 2, 2017), https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5_story.html?utm_term=.a423f01e03b1, archived at <https://perma.cc/8U7U-ZH7X>. For a discussion on NERC, see *infra* Part II B.

43. *Id.*

44. Eilperin & Entous, *supra* note 41.

45. *Id.*

46. *Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector*, U.S. DEP'T OF HOMELAND SEC. 1, 1 (Jan. 27, 2016), <https://www.documentcloud.org/documents/2785293-DHS-27-1-2016-Intelligence-Assessment.html>, archived at <https://perma.cc/8FB8-LR9E> [hereinafter *Damaging Cyber Attacks*].

47. *Id.* at 2.

48. *Id.*

49. See Pagliery, *Government reveals*, *supra* note 40.

50. *Id.*

services only in the event of hostilities between their nations and the U.S., and that a “cyberattack[] against the American energy sector is ‘possible but not likely.’”⁵¹

Not all threats to the nation’s energy infrastructure are done by hackers. On August 14, 2003, there was a major blackout affecting eight states in the Northeast, and part of Canada, leaving approximately 50 million people without power for two days.⁵² After a three-month investigation, conducted jointly by the U.S. and Canada, a report was released stating the blackout was caused by human error and equipment failures.⁵³ The blackout occurred when the summer heat caused a powerline to sag and brush against some overgrown trees in Ohio, resulting in the powerline shutting down.⁵⁴ This would normally set off an alarm at the utility company, but the alarm failed, and as system operators were working to figure out what had happened, three other lines also shut down, forcing other power lines to carry the extra burden of supplying power, which ultimately resulted in the lines shutting down, triggering failures throughout the U.S. and Canada.⁵⁵ In the end, it was determined four main factors caused the blackout,⁵⁶ and 46 recommendations were made to reduce the threat of future blackouts.⁵⁷

In 2017 the Department of Homeland Security and the FBI released an “amber” alert report to companies operating nuclear power plants in the U.S. warning against malware attacks aimed at the employees of nuclear companies.⁵⁸ The report noted that no nuclear plants were in danger, and that the attempted hacks were focused on the personal computers of employees.⁵⁹ This warning came after an earlier warning from DHS in 2017 about possible cyberattacks on the energy sector, as well as the healthcare industry, communications, and public health.⁶⁰ While the reports and warnings indicate that the energy infrastructures of the U.S. have not been affected yet, it seems only a matter of time before hackers gain access.

51. *Id.*

52. See James Barron, *The Blackout of 2003: The Overview; Power Surge Blacks Out Northeast, Hitting Cities in 8 States and Canada; Midday Shutdowns Disrupt Millions*, N.Y. TIMES (Aug. 15, 2003), <http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html>, archived at <https://perma.cc/A9RZ-MPHX>; J.R. Minkel, *The 2003 Northeast Blackout -- Five Years Later*, SCI. AM. (Aug. 13, 2008), <https://www.scientificamerican.com/article/2003-blackout-five-years-later/>, archived at <https://perma.cc/82SW-R4A5>.

53. Minkel, *supra* note 52.

54. *Id.*

55. *Id.*

56. See 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 18 (2004), <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>, archived at <https://perma.cc/R5BX-6DMU> (the four causes of the blackout were: a “fail[ure] to assess and understand the inadequacies of [the] system,” “[i]nadequate situational awareness,” “fail[ure] to manage [] tree growth,” and “[f]ailure of the interconnected grid’s reliability organizations to provide effective real-time diagnostic support”).

57. See U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE IMPLEMENTATION OF THE TASK FORCE RECOMMENDATIONS 4 (2006), <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf>, archived at <https://perma.cc/2K3A-DWCE> (final report discussing all forty-six recommendations made by the task force).

58. Sean Gallagher, *FBI-DHS “amber” alert warns energy industry of attacks on nuke plant operators*, ARS TECHNICA (July 6, 2017, 11:20 PM), <https://arstechnica.com/information-technology/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/>, archived at <https://perma.cc/E52M-ER7X>.

59. *Id.*

60. See U. S. COMPUTER EMERGENCY READINESS TEAM, ALERT (TA17-117A), INTRUSIONS AFFECTING MULTIPLE VICTIMS ACROSS MULTIPLE SECTORS (2017), <https://www.us-cert.gov/ncas/alerts/TA17-117A>, archived at <https://perma.cc/3DGL-F6AQ>.

II. CURRENT PROTECTIONS TO THE ENERGY INFRASTRUCTURE

A. Federal Energy Regulatory Commission and the Office of Energy Infrastructure Security

The only federal agency that can set standards governing cybersecurity for the electric utility industry is the Federal Energy Regulatory Commission (FERC).⁶¹ FERC is composed of 12 offices, one being the Office of Energy Infrastructure Security (OEIS).⁶² OEIS “provides leadership, expertise and assistance to [FERC] to identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks”⁶³ OEIS is responsible for “formulat[ing] and mak[ing] recommendations for [FERC] action and undertak[ing] collaborative engagement with other federal and state agencies and the energy industry to work to identify and communicate risks and vulnerabilities to this nation’s energy infrastructure”⁶⁴ OEIS focuses on:

Developing recommendations for identifying, communicating and mitigating potential cyber and physical security threats and vulnerabilities . . . ; Providing assistance, expertise and advice to other federal and state agencies . . . in identifying, communicating and mitigating potential cyber and physical threats and vulnerabilities . . . ; Participating in interagency and intelligence-related coordination and collaboration efforts with appropriate federal and state agencies and industry representatives on cyber and physical security matters . . . ; Conducting outreach with private sector owners, users and operators of energy delivery systems regarding identification, communication and mitigation of cyber and physical threats. . . .⁶⁵

B. North American Electric Reliability Corporation

North American Electric Reliability Corporation (NERC) is a not-for-profit organization, founded in 1968 to develop and promote voluntary compliance with the rules for a reliable power grid in North America.⁶⁶ The purpose of NERC is to ensure the power systems of North America remain reliable and secure.⁶⁷ NERC is responsible for developing and enforcing reliability standards; assessing and monitoring the energy systems; and educating, training, and certifying industry workers.⁶⁸ The

61. Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission*, 41 N. KY. L. REV. 437, 437 (2014).

62. *About FERC*, FERC, <https://www.ferc.gov/about/about.asp>, archived at <https://perma.cc/QA3W-DHSM> (last visited Aug. 16, 2018).

63. *Office of Energy Infrastructure Security (OEIS)*, FERC, <https://www.ferc.gov/about/offices/oeis.asp>, archived at <https://perma.cc/VD5C-DLLH> (last visited Aug. 16, 2018).

64. *Id.*

65. *Id.*

66. *About NERC*, NERC, <https://www.nerc.com/AboutNERC/Pages/default.aspx>, archived at <https://perma.cc/GL22-QE6G> (last visited Aug. 16, 2018); *FAQ*, NERC, <https://www.nerc.com/AboutNERC/exec/Pages/FAQ.aspx>, archived at <https://perma.cc/8U4D-WGJQ> (last visited Dec. 2, 2018).

67. *About NERC*, *supra* note 66; *FAQ*, *supra* note 66.

68. *About NERC*, *supra* note 66.

U.S., Canada, and parts of northern Mexico make up NERC's area of coverage.⁶⁹ NERC is overseen by FERC as the electronic reliability organization for the U.S.⁷⁰

One department within NERC is the Electricity Information Sharing and Analysis Center (E-ISAC) which "establish[es] [] situational awareness, incident management, coordination, and communication capabilities within the [e]lectricity [s]ector"⁷¹ E-ISAC works with the Department of Energy (DOE) and the Electricity Subsector Coordinating Counsel to help the industry "prepare for and respond to cyber and physical threats, vulnerabilities, and incidents."⁷² NERC has several committees to help achieve its objectives; one being the Critical Infrastructure Protection Committee (CIPC) which helps NERC improve the electricity infrastructure from cyberattacks.⁷³

C. Energy Policy Act

After the blackout in the northeast in 2003,⁷⁴ Congress enacted the Energy Policy Act of 2005 (EPAAct).⁷⁵ Among other things, EPAAct gives FERC the power "to establish a program to ensure the reliability of the U.S. 'Bulk-Power System' (i.e., the nation's electric grid) by setting standards to apply to the users, owners, and operators of that system."⁷⁶ The EPAAct increased the number of organizations subject to FERC's jurisdiction from 200 to over 1,500.⁷⁷ The Act also created hefty penalties for violating FERC's standards, some as high as \$1 million a day.⁷⁸

D. Code of Federal Regulations

i. Protection of Digital Computer and Communications Systems

A federal regulation covering the protection of digital computer and communication systems and networks, mandates energy providers protect all computer and communications systems and networks from cyberattacks.⁷⁹ Providers must protect the systems from cyberattacks that could "[a]dversely impact the integrity or confidentiality of data and/or software; [d]eny access to systems, services, and/or data;

69. *Id.*

70. *Id.*

71. Letter from Patricia Hoffman, Ass't Sec'y, U.S. Dep't of Energy, to Gerry Cauley, President & CEO, N. Am. Elec. Reliability Corp., (Mar. 14, 2013) (on file with the U.S. Dep't of Energy).

72. *Electricity ISAC*, NERC, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>, archived at <https://perma.cc/7YH8-2JEZ> (last visited Aug. 16, 2018).

73. For more information on the CIPC and the other committees of NERC, see *Standing Committees and Other*, NERC, <http://www.nerc.com/comm/Pages/default.aspx>, archived at <https://perma.cc/3SXA-8ZCR> (last visited Aug. 16, 2018); *Critical Infrastructure Protection Committee (CIPC)*, NERC, <https://www.nerc.com/comm/CIPC/Pages/default.aspx>, archived at <https://perma.cc/K4PR-53T7> (last visited Dec. 2, 2018).

74. See *supra* Part I C.

75. Court, *supra* note 61, at 437-38. To view the full act, see Energy Policy Act of 2005, 42 U.S.C. §§ 15801-16524 (2012).

76. Court, *supra* note 61, at 438.

77. *Id.*

78. *Id.*

79. Protection of Digital Computer and Communication Systems and Networks, 10 C.F.R. § 73.54 (2018).

and [a]dversely impact the operation of systems, networks, and associated equipment.”⁸⁰ This shall be accomplished by analyzing and identifying what must be protected from cyberattacks by “[e]stablish[ing], implement[ing], and maintain[ing] a cyber security program,” and “[i]ncorporat[ing] the cyber security program.”⁸¹ The regulation requires a cyber security plan be developed and “must describe how the requirements . . . will be implemented . . .” and “must include measures for incident response and recovery for cyber attacks.”⁸² This security plan must describe how the energy provider will: “Maintain the capability for timely detection and response to cyber attacks; [m]itigate the consequences of cyber attacks; [c]orrect exploited vulnerabilities; and [r]estore affected systems, networks, and/or equipment affected by cyber attacks.”⁸³

ii. Networks and Cyber Security Event Notifications

Another federal regulation, Networks and Cyber Security Event Notifications, sets requirements for what to do in the event of an actual or suspected cyberattack.⁸⁴ Upon the discovery of a cyberattack, the provider must call the Nuclear Regulatory Commission’s Headquarters Operations Center, and then “submit a written security follow-up report . . . within 60 days of the []phone notification. . . .”⁸⁵ The time for notification varies depending on the severity of the attack. Notification must be made within one hour after discovery if the attack had an adverse impact; within four hours if the attack could have had an adverse impact; and within eight hours after receiving information that someone may have been trying to gather information to conduct a cyberattack.⁸⁶ The provider is also required to use their site corrective action plan within 24 hours of discovery to “record vulnerabilities, weaknesses, failures and deficiencies in their [] cyber security program.”⁸⁷

III. CYBERSECURITY AND ENERGY INDUSTRIES

A. Nuclear Power

Of the four industries discussed in this note, nuclear power is perhaps the most protected from cyber threats. The Nuclear Regulatory Commission (NRC) is the overseeing authority of the nuclear industry and is responsible for the creation of policies and regulations relating to the nuclear industry.⁸⁸ After the terrorist attacks of September 11, 2001, the NRC ordered nuclear power plants to enhance security in multiple areas, including cybersecurity.⁸⁹

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.*

84. Cyber Security Event Notifications, 10 C.F.R. § 73.77 (2018).

85. *Id.*

86. *Id.*

87. *Id.*

88. *See* UNITED STATES NUCLEAR REGULATORY COMMISSION, OVERVIEW <https://www.nrc.gov/docs/ML1616/ML16165A342.pdf>, archived at <https://perma.cc/39W3-82PU>.

89. *Cyber Security for Nuclear Power Plants*, NUCLEAR ENERGY INST., (July 2016), <https://www.nei.org/resources/reports-briefs/cybersecurity-for-nuclear-power-plants> archived at <https://perma.cc/8H85-NMPB>.

Nuclear power plants are protected from cyberattacks by layers of safety precautions, with the first line of defense being isolation.⁹⁰ What this means is that the “[c]ritical safety and security systems at nuclear energy facilities are isolated from the internet. They have no direct access to web, nor do they have indirect access because they are not connected to the plants’ internal networks.”⁹¹ Another layer of protection is NRC’s requirement that nuclear plants be designed to safely shut down and remain cooled if the systems detect any abnormalities on the electric grid.⁹² Some steps nuclear power plants have taken to protect against cyber threats include: “[i]solat[ing] key control systems;” “[e]nhanc[ing] and implement[ing] strict controls over the use of portable media and equipment;” and “[p]erform[ing] detailed cyber security assessments.”⁹³

Despite all of the layers of protection in the nuclear industry, it is still vulnerable to cyberattacks. In January 2003, the Davis-Besse nuclear power plant in Oak Harbor, Ohio fell victim to one of the first cyberattacks of a nuclear power plant.⁹⁴ The attack started when workers noticed the company’s network seemed to be running slow, or lagging, and by the afternoon malware had entered the systems used to control the nuclear reactor.⁹⁵ The plant’s Safety Parameter Display System, which gives operators information about the state of the plant, shut off, and then the computers crashed.⁹⁶ The reactor was offline at the time of the attack, and everything was restored after a few hours.⁹⁷

One step the nuclear power industry can do to protect itself from cyberattacks is to assess the cyber threats and develop guidelines to measure these threats.⁹⁸ Human factors in cybersecurity should also be addressed as the systems most likely to succumb to failure are the ones relying on human actions and interactions.⁹⁹ Nuclear power plants should share information obtained from actual cyberattacks and attempted ones, with nuclear plants in the U.S. and around the world.¹⁰⁰ Another area that could be improved in the nuclear industry to protect against cyberattacks is with the communication between the nuclear technicians and information technology experts.¹⁰¹ Nuclear power plants also need to be able to track the integrity of their data, to ensure nothing has been “tampered with by a manufacturer, a consumer, a user, or a third-party developer.”¹⁰²

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. Jason Deign, *7 Ways to cyber-secure a nuclear power plant*, CISCO (Jul. 20, 2016), <https://newsroom.cisco.com/feature-content?articleId=1774597&type=webcontent>, archived at <https://perma.cc/Z9RN-R5QK>.

95. *Id.*

96. *Id.*

97. *Id.* The malware that infected Davis-Besse’s networks was a worm called SQL Slammer. After being dormant for a decade, SQL Slammer has recently made a comeback, re-entering into the news. See Ionut Arghire, *SQL Slammer Worm Crawls Back*, SEC. WEEK (Feb. 3, 2017), <http://www.securityweek.com/sql-slammer-worm-crawls-back>, archived at <https://perma.cc/Z9RN-R5QK>; Darren Pauli, *Slammer work slithers back online to attack ancient SQL servers*, THE REGISTER (Feb. 5, 2017, 11:29 PM), https://www.theregister.co.uk/2017/02/05/sql_slammer_back/, archived at <https://perma.cc/MP92-QERN>.

98. Deign, *supra* note 94.

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

B. Hydropower

In the hydropower industry, the hydro facilities are often located in the middle of nowhere, are generally unmanned, and require remote monitoring and controlling.¹⁰³ Many of the computer systems controlling hydropower facilities are old and outdated and are often connected to office computers which are fairly easy to hack.¹⁰⁴ If someone were to gain access to a hydropower facility's computers, they could potentially cause flooding.¹⁰⁵

In 2013, Iranian hackers successfully hacked into the control system of Bowman Avenue Dam near the village of Rye Brook, New York, located about 20 miles from New York City.¹⁰⁶ While the specific details of this cyberattack are still classified, federal authorities discovered the attack while monitoring computers linked to possible Iranian hackers, and at first thought the cyberattack had occurred at another, much larger dam with a similar name.¹⁰⁷ Officials, at first, thought the dam hacked was the Arthur R. Bowman Dam in Oregon, which is a 245-foot tall earthen dam, but the dam actually hacked was the Bowman Avenue Dam, which is a 20-foot tall concrete slab across Blind Brook, and was originally used for ice production.¹⁰⁸ The hackers did not take control of the system, but only probed it, obtaining water level information and temperatures, but could have been able to open the floodgate remotely, if it had not been down for maintenance at the time of the incident.¹⁰⁹ Because most of the hydropower industry's control systems are similar to those at the Bowman Avenue Dam, this incident shows how vulnerable the hydropower industry is to cyberattacks.¹¹⁰

C. Solar Power

Similar to hydropower, federal authorities are generally tight lipped about the cybersecurity of solar power panels and facilities. The Manhattan Institute released a study in 2016, where they found "that making the power grid networked enough to handle the intermittent and unreliable nature of solar and wind power inherently makes it more vulnerable to cyberattacks."¹¹¹ The study also noted the amount of money the government spends on securing the nation's energy infrastructures is trivial compared to what the government spends on promoting green energy such as solar power.¹¹²

103. Max Kutner, *Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure*, NEWSWEEK (Mar. 30, 2016, 8:12 AM), <http://www.newsweek.com/cyber-attack-rye-dam-iran-441940>, archived at <https://perma.cc/9PG4-FP2U>.

104. Danny Yadron, *Iranian Hackers Infiltrated New York Dam in 2013; Cyberspies had Access to Control System of Small Structure Near Rye in 2013, Sparking Concerns that Reached to the White House*, WALL ST. J., Dec. 21, 2015, FACTIVA.

105. *Id.*

106. *Id.*

107. *Id.* (there are 31 dams in the U.S. with "Bowman" in the name).

108. *Id.*

109. *Id.*; Kutner, *supra* note 103.

110. Kutner, *supra* note 103.

111. Andrew Follett, *Security Expert: Solar Panels are Easy to Hack*, THE DAILY CALLER (Aug. 2, 2016, 4:14 PM) <http://dailycaller.com/2016/08/02/security-expert-solar-panels-are-extremely-easy-to-hack/?pring=1>, archived at <https://perma.cc/D64Q-3GG4>.

112. *Id.*

One California citizen decided to test the security of his newly installed solar panels, and what he found was disturbing.¹¹³ He first found an open Wi-Fi access point coming from his solar provider's Management Unit, and his computer was able to guess the username and password—"admin" and "support."¹¹⁴ Once in the system, he could have made changes to the panels' configuration and could have shut down the solar power system.¹¹⁵ He also found access to a virtual private network to all of the solar devices produced by one manufacturer, which would have allowed him to control anyone's solar panels, and if these panels were connected to other home networks, he would have had access to those as well.¹¹⁶ This example proves what experts fear—solar panels can be easy to hack—giving hackers the ability to knock them offline; cause them to overheat, causing physical damage to the panels themselves; and allowing hackers to have access to personal home networks.¹¹⁷

D. Wind Power

Wind farms are considered to have some of the most current, sophisticated security methods in place to protect against cyberattacks.¹¹⁸ The power conversion equipment used in wind turbines "provides a buffer between the generator and the bulk power system that is absent in almost all other types of power plants," making wind farms one of the most sophisticated in the energy industry.¹¹⁹ This power conversion equipment used in the wind industry also protects from abnormal voltage and frequency deviations, providing an additional layer of protection against cyberattacks.¹²⁰ Because of the competitive nature of the wind industry, wind farm operators have financial motivators to ensure their plants are secure from competitors gaining access to commercially sensitive information, which also provides protection against cyberattacks.¹²¹ However, one possible flaw in the wind energy industry is wind turbine "[s]oftware development information is publicly searchable and, technically, open to everyone"¹²²

Despite the wind industry being considered one of the most sophisticated in the energy industry, it has vulnerabilities. In March 2015, a German researcher found a vulnerability that could allow anyone to hack into several types of wind turbines, potentially giving hackers the power to shut the turbines down.¹²³ One of the easiest

113. Thomas Brewster, *This Man Hacked His Own Solar Panels . . . And Claims 10,000 More Homes Vulnerable*, FORBES (Aug. 1, 2016, 10:00 AM), <https://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers/>, archived at <https://perma.cc/M9HA-X3EB>.

114. *Id.*

115. *Id.*

116. *Id.*

117. Follett, *supra* note 111.

118. Paul Dvorak, *Cyber security and wind-farm penetrations*, WIND POWER ENG'G (Oct. 21, 2015), <http://www.windpowerengineering.com/uncategorized/cyber-security-and-wind-farm-penetrations/>, archived at <https://perma.cc/V8SD-AQC4>.

119. David Ward, *Fact Check: Wind plant owners are leaders in cyber-security and grid reliability*, INTO THE WIND: THE AWEA BLOG (Jul. 3, 2014), <http://www.aweablog.org/fact-check-wind-plant-owners-are-leaders-in-cyber-security-and-grid-reliability>, archived at <https://perma.cc/W3GP-58XV>.

120. *Id.*

121. *Id.*

122. Dvorak, *supra* note 118.

123. See Thomas Brewster, *Hundreds of Wind Turbines and Solar Systems Wide Open To Easy Exploits*, FORBES (June 12, 2015, 12:37 PM), <https://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar->

ways hackers gain access to energy infrastructure systems, such as wind turbines, is by successfully guessing user login information and passwords. One report stated administrators often “use default, generic, and surprisingly easy passwords to protect” their systems, which makes accessing the system much easier for hackers trying to get in.¹²⁴

IV. PROPOSED LEGISLATION

A. Proposed Bill: Grid Cybersecurity Research and Development Act

The House of Representatives introduced a bill “to provide for a comprehensive interdisciplinary research and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks” in October 2017.¹²⁵ This Bill would help to identify risks in the nation’s energy sector, develop methods to detect cyber hackers, and develop technology to protect the energy sector from cyberattacks.¹²⁶ This Act would require the government to “work with manufacturers to build or retrofit security features and protocols.”¹²⁷

Since being proposed in October 2017, it has been referred to several committees and subcommittees, the most recent being the subcommittee on Research and Technology in May 2018.¹²⁸ The costs of this proposed Act begin with a cost of \$65 million the first year, increasing each year, to \$79 million the fifth year.¹²⁹

B. Proposed Bill: Securing Energy Infrastructure Act

In January 2017 a bill was introduced to the Senate and referred to the Committee on Energy and Natural Resources to establish “a pilot program to identify security vulnerabilities of certain entities in the energy sector.”¹³⁰ If enacted, this Bill would require a two-year pilot program to be started within 180 days of the date of enactment.¹³¹ The purpose of this program would be to “identify new classes of security vulnerabilities” within the energy sector, and “to isolate and defend industrial control systems of covered entities from security vulnerabilities.”¹³² One sponsor of this Bill calls it “a ‘retro’ approach” because it would revert some security devices on the grid

systems-is-easy/#50ff0e5d4d5c, *archived* at <https://perma.cc/U5U6-57BR>; Lorenzo Franceschi-Biccieri, *Some Wind Turbines Can Be Hacked by Anyone With an Internet Connection*, MOTHERBOARD (Apr. 3, 2015, 8:30 AM), https://motherboard.vice.com/en_us/article/some-wind-turbines-can-be-hacked-by-anyone-with-an-internet-connection, *archived* at <https://perma.cc/VB9P-P887>.

124. Dvorak, *supra* note 118.

125. *See* Grid Cybersecurity Research and Development Act, H.R. 4120, 115th Cong. (2017).

126. *Id.*

127. *Id.*

128. STAFF OF COMM. ON SCI., SPACE, & TECH., 115TH CONG., BILL TRACKING REP. (Comm. Doc. 2018).

129. H.R. 4120.

130. Securing Energy Infrastructure Act, S. 79, 115th Cong. (2017).

131. *Id.*

132. *Id.*

back “to analog and human-operated systems instead of connecting them to computers.”¹³³ The funds authorized for the completion of the pilot program are \$10 million.¹³⁴

The Bill would also establish a working group “to evaluate the technology platforms and standards used in the [pilot] [p]rogram” and “to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.”¹³⁵ The Secretary of Energy (Secretary) will appoint the members of the working group, which will consist of no fewer than ten members.¹³⁶ These members will come from the DOE, the energy industry, and the DHS, among others.¹³⁷

Within two years of the first disbursement of funds, the Secretary will submit a final report on the pilot program to Congress that will: “describe[] the results of the Program; include[] an analysis of the feasibility of each method studied under the Program; and describe[] the results of the evaluation conducted by the working group.”¹³⁸ The funds authorized for the working group and final report are \$1.5 million.¹³⁹ Senator Angus King, who introduced the bill to the Senate, said, “I don’t know how many warnings we have to get before something catastrophic happens. That’s why I introduced this bill . . . that [it] is a bipartisan bill aimed at trying to determine what some of the ways are to protect the grid.”¹⁴⁰

C. Proposed Resolution: Establishing the Select Committee on Cybersecurity

A resolution was introduced to the Senate in January 2017 requesting the establishment of the Select Committee on Cybersecurity.¹⁴¹ One of the resolution’s sponsors, Senator Cory Gardner, said, “Cybersecurity policy is one of the most complex and significant challenges facing Congress, yet the Senate’s structure to investigate and address cyber issues is diffuse and inadequate. This has led to an uncoordinated policy response to recent cyberattacks on government agencies, businesses, and infrastructure.”¹⁴² This proposed committee would be composed of 21 members, be responsible for overseeing and holding continuing studies on cybersecurity threats, and to make recommendations regarding these threats.¹⁴³ “All proposed legislation, messages, petitions, memorials, and other matters relating to the following” must be

133. Jacqueline Toth, *Grid Cybersecurity Measure Would Examine Benefits of Analog Systems*, CQ ROLL CALL, Jan. 11, 2017, 2017 WL 103845.

134. S. 79.

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.*

140. Jeremy Dillon, *As Grid Cybersecurity Fears Grow, Senate Measure Eyes Broad Approach*, CQ ROLL CALL, Jan. 30, 2017, 2017 WL 393335.

141. Establishing the Select Committee on Cybersecurity, S. Res. 23, 115th Cong. (2017).

142. Dillon, *supra* note 140.

143. For a list of the 21 committee members, see S. Res. 23.

referred to the Select Committee on Cybersecurity: “[d]omestic and foreign cybersecurity risks,” and the “[a]uthorizations for appropriations . . . for preventing, protecting against, or responding to cybersecurity threats to the United States.”¹⁴⁴

The committee will be authorized to make investigations, hold hearings, subpoena witnesses, take depositions, hire consultants, and make recommendations on matters within its jurisdiction.¹⁴⁵ The committee shall be able to obtain necessary information related to cybersecurity threats to ensure they have complete and up to date information.¹⁴⁶ Annual reports on cyber threats will be provided to the committee from the Directors of National Intelligence, the Central Intelligence Agency, and the Federal Bureau of Investigation, as well as the Secretary of Defense and the Secretary of State.¹⁴⁷

D. Failed Proposal: Amendment to the Federal Power Act

If previous attempts to protect the nation’s energy infrastructure are an indicator of the success or failure of the currently proposed bill and resolution, then the future of these proposals is bleak. In April 2015, a bill was proposed “to protect the bulk-power system from cyber security threats.”¹⁴⁸ This Bill had recommended adding a section covering cybersecurity threats to the Federal Power Act.¹⁴⁹ This amendment would have allowed the Secretary—with written notice from the President “that immediate action is necessary to protect the bulk-power system from a cyber security threat,”—to require “any entity that owns, controls, or operates a bulk-power system facility to take such actions as the Secretary determines will best avert or mitigate the cyber security threat.”¹⁵⁰ The Secretary would also have been encouraged to consult with officials in Canada and Mexico to protect the electricity grid from cyber threats.¹⁵¹ Congress adjourned before this bill passed any of the committees, and therefore this proposed amendment to the Federal Power Act failed.¹⁵²

E. Failed Proposal: Grid Cybersecurity Research and Development Act

In September 2016, another bill, the Grid Cybersecurity Research and Development Act, was proposed to the House of Representatives to “provide for a comprehensive interdisciplinary research and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks.”¹⁵³ In this proposed Act, the Secretary would have carried out a “research, development, and demonstration initiative to harden and mitigate the electric grid from the consequences of cyber

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. S. 1068, 114th Cong. § 224 (2015).

149. *Id.*

150. *Id.*

151. *Id.*

152. *S. 1068 (114th): A bill to amend the Federal Power Act to protect the bulk-power system from cyber security threats*, GOVTRACK (last visited Nov. 14, 2018, 12:45 PM), <https://www.govtrack.us/congress/bills/114/s1068> [hereinafter GOVTRACK, S. 1068].

153. Grid Cybersecurity and Research and Development Act, H.R. 6227, 114th Cong. (2016).

attacks by increasing the cyber security capabilities of the electricity sector and accelerating the development of cybersecurity technologies and tools.”¹⁵⁴

The Secretary would have been responsible for, among other things, “identify[ing] cybersecurity risks to the communication and control systems,” “develop[ing] methods and tools to rapidly detect cyber intruders,” and “develop[ing] secure industrial control system protocols.”¹⁵⁵ The Secretary would have also been responsible for updating several cybersecurity publications, and for “develop[ing] voluntary guidance to improve forensic analyses capabilities, including developing standardized terminology and monitoring processes; identifying minimum data needed; and utilizing human factors research to develop more effective procedures for logging incident events”¹⁵⁶ Under this Act, the Secretary would have worked with the private owners and operators of the energy sector to conduct “voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems; [and to] develop cybersecurity risk assessment tools and provide confidential analyses and recommendations.”¹⁵⁷ This act would have developed both “assessment methods and tools to identify existing personnel that show competence in [] core skills,” and “cybersecurity training and retraining standards, lessons, and recommendations for the electricity sector that minimize duplication of cybersecurity compliance training programs.”¹⁵⁸

The Secretary would have been required to collaborate with the Secretary of Homeland Security, other Federal agencies, and the energy sector to “conduct a study to analyze cyberattacks on electricity sector industrial control systems and identify cost-effective opportunities to improve cybersecurity.”¹⁵⁹ Like the proposed amendment to the Federal Power Act, Congress adjourned before this Bill passed any of its assigned committees, and therefore the Grid Cybersecurity Research and Development Act failed.

V. RECOMMENDATIONS

A. Does the Current and Proposed Legislation Go Far Enough?

Given the successful hacking attempts to the nation’s energy infrastructure across several industries, it is apparent that current legislation does not go far enough in protecting against cyberattacks.¹⁶⁰ Both the proposed amendment to the Federal Power Act in 2015, and the Grid Cybersecurity Research and Development Act of

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.* For an explanation on Red team-blue team exercises, see *infra* Part V C. See also Pierluigi Paganini, *Cyber Security: Red Team, Blue Team and Purple Team*, SEC. AFFAIRS (Jul. 23, 2016) <http://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html>, archived at <https://perma.cc/T8LK-XMKC>. See also Tech Insider, *Watch Hackers Break into the US Power Grid*, YOUTUBE (May 11, 2016), <https://www.youtube.com/watch?v=pL9q2lOZ1Fw>, archived at <https://perma.cc/Ry69-EXRX> (a group known as Red Team Security, hired by a power company, successfully hacks into the power company’s systems).

158. H.R. 6227.

159. *Id.*

160. See *supra* Part III A, B, and C.

2016 failed after being sent to committees for review.¹⁶¹ This is where most proposed bills and amendments die. For a proposed piece of legislation to become law, it must pass both houses and have approval from the President.¹⁶² Once a bill or amendment has been introduced to the house or senate, it is then sent to committees to be voted on, but unfortunately many bills die before voting because many bills are often ignored by their assigned committees.¹⁶³

One problem with the Grid Cybersecurity Research and Development Act is that it was simply a research proposal, which would take private sector energy operators and allow them to voluntarily participate. The information gathered from this research study would not have involved all operators and therefore could have lacked vital information when conducting the study.¹⁶⁴ In a study set up this way, some sectors, such as the wind industry, may not have had a lot of participation since this industry tends to keep information secret from competitors.

One possible issue with the pilot program proposed in January 2017, is that it involves a two-year pilot program to identify security vulnerabilities in the energy industry, however, cyberattacks are constantly evolving—as technology advances, so do the techniques of hackers. Because it takes so long to enact laws and regulations, by the time the study is completed, and recommendations are considered and enacted, the entire cyber community could completely change, making anything discovered during the pilot program obsolete.

The establishment of a Select Committee on Cybersecurity may be able to pass both houses. Having a committee specifically designated to handle cybersecurity threats and issues could be beneficial to protect from cyberattacks. The committee would need to consist of people with knowledge in the energy industry, as well as in cybersecurity, and hacking. Giving this committee the ability to gather the information needed to make the most accurate and reliable recommendations possible will be crucial for its success. Requiring an annual report would hold the committee responsible, however, it may be good to also require them to release individual reports on known cyberattacks within a certain time frame, in addition to the annual report.

B. Other Options

Instead of establishing a Select Committee on Cybersecurity, however, Congress could use NERC's CIPC. This committee has several subcommittees, task forces, and work groups already dedicated to protecting the infrastructure from cyberattacks.¹⁶⁵ By utilizing an already existing committee, the government could potentially save money and gain valuable knowledge from an already established group.

161. See GOVTRACK, S. 1068, *supra* note 152; H.R. 6227 (114th): *Grid Cybersecurity Research and Development Act*, GOVTRACK (last visited Nov. 14, 2018, 12:45 PM), <https://www.govtrack.us/congress/bills/114/hr6227> archived at <https://perma.cc/W7TZ-H962>.

162. See *Why Do so Few Bills Become Law?*, REFERENCE, <https://www.reference.com/government-politics/bills-become-laws-d071997480e11fee> (last visited Aug. 16, 2018), archived at <https://perma.cc/9URF-3CNZ>.

163. *Id.*

164. See generally H.R. 6227 (the only required members are members from Federal agencies).

165. For more information on the 20 subcommittees, task forces, and work groups under the CIPC, see *Critical Infrastructure Protection Committee (CIPC)*, NERC, <http://www.nerc.com/comm/CIPC/Pages/default.aspx>, archived at <https://perma.cc/L42F-4JGF> (last visited Aug. 16, 2018).

The government should also establish federal regulations covering the education and training of industry workers using the CIPC's structure. The five key methods the CIPC uses to educate and train industry workers are: "[p]rotecting," "[d]eterring," "[p]reventing," "[l]imiting," and "[r]ecovering."¹⁶⁶

C. Industries Can Take Action

While waiting for the government to enact better protections against cyberattacks for the nation's energy infrastructures, there are some things industries can do to protect themselves now. These include: sending out phishing test emails, conducting employee training, and hiring companies to hack into their own systems.

Phishing occurs when a hacker sends out an email that appears to be from a business or employer with the intention of tricking the recipient into giving out their personal or login information.¹⁶⁷ An estimated 156 million phishing emails are sent out daily, with 80,000 people falling victim to them.¹⁶⁸ Companies can protect themselves by sending out their own phishing test emails. To do this, companies would need to send out a phishing email to all employees, and then document which employees clicked the link provided, or opened the document attached.¹⁶⁹ For the best results, information about the company induced phishing attack should be shared with all employees, providing information on how many failed versus how many passed the phishing test, and explaining the damages that could have occurred from those who fell victim to the fake attack.¹⁷⁰

Training employees to spot phishing attempts is one way to prevent cyberattacks since many hackers gain access by phishing.¹⁷¹ Other methods to protect from cyberattacks include requiring employees to use strong, unique passwords that cannot be easily guessed.¹⁷² The "see something, say something" motto the country has adopted in its battle against terrorism, can also be used to protect companies from cyberattacks. If an employee finds or suspects a problem, or if they feel they may have clicked something that could have been a phishing attempt or downloaded a suspicious file, they should be trained to report it right away. This could help detect an attack as soon as it happens, making it easier to stop before the hacker gains much, if any information.¹⁷³

Perhaps the best way an energy company can protect itself from cyberattacks, is by hiring a company to hack into its systems. This is often called red team-blue team

166. *Id.*

167. *Phishing*, FED. TRADE COMM'N, <https://www.consumer.ftc.gov/articles/0003-phishing>, archived at <https://perma.cc/VSR7-QXBN> (last visited Aug. 16, 2018). To see an example of what a phishing email might look like, see *Protect yourself from phishing*, MICROSOFT, <https://support.microsoft.com/en-us/help/4033787/windows-protect-yourself-from-phishing>, archived at <https://perma.cc/R8CG-7V54> (last visited Nov. 25, 2018).

168. Austin Whipple, *If You're Not Phishing Your Employees, You Should Be: Here's How*, BETTER CLOUD MONITOR (June 9, 2016), <https://www.bettercloud.com/monitor/internal-phishing-training/>, archived at <https://perma.cc/9PXU-U2CL>.

169. *Id.*

170. *Id.*

171. Juan Martinez, *6 Ways to Train Your Employees to Prevent Cyberattacks*, PC MAG (Oct. 21, 2016, 4:20 PM), <http://www.pcmag.com/article/348925/6-ways-to-train-your-employees-to-prevent-cyberattacks>, archived at <https://perma.cc/75G4-PDMT>.

172. *Id.*

173. *Id.*

exercises and was one of the testing methods recommended in the 2016 proposed comprehensive interdisciplinary research and development initiative to protect against cyberattacks to the energy sector.¹⁷⁴ Red team-blue team exercises come from military jargon, and are basically composed of a group of professionals (the red team), which does everything they can to attack the energy company (the blue team), while the energy company tries to defend themselves.¹⁷⁵

CONCLUSION

With the world's eyes suddenly opened to the reality of cyberattacks, many people are now concerned about, and focusing on ensuring the energy infrastructures of the U.S. are secure. Hackers attempt to penetrate the system every day, it can take months to learn someone has gained access, and once inside, they can do insurmountable damage. While the potential damage that can be done varies by industry—nuclear melt down, flooding, home network hacking, simply turning the lights off—the methods of gaining access are very similar.

These scary realities are just one reason why our current legislation should push to ensure we enact more laws to better protect the energy infrastructures. The current protections are a step in the right direction, but more is needed. The proposed Select Committee on Cybersecurity would be one step in the right direction, as it would create a committee solely designated to investigating cyberattacks to the energy grid, but this does not go far enough to protect our energy infrastructures from cyberattacks.

One weakness in each of the four sectors covered in this note, was the potential for malware to enter into computer systems. Once hackers gain access to the system, they often sit quietly, monitoring the daily operations until they are ready to strike. This ability to essentially spy on an energy provider for months, without ever being detected, makes the need for better cybersecurity regulations even more crucial. Hackers are trying to gain access to the energy grid on a daily basis, and as one hacker for a red team security group said, “We will get in, there's no doubt about it,”¹⁷⁶ it is simply a matter of time.

174. See *supra* Part IV E.

175. Doug Drinkwater & Kacy Zurkus, *Red team versus blue team: How to run an effective simulation*, CSO (Jul. 26, 2017, 4:03 AM), <http://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html>, archived at <https://perma.cc/CWQ7-ZZHA>. To watch a video of a Red Team Security group successfully break into the energy grid, see Tech Insider, *supra* note 157.

176. Tech Insider, *supra* note 157.