Fiddling with the Switch: Why Critical Infrastructure Protection Standard CIP-008-6 Should Be Adjusted to Achieve Its Goal of Maintaining and Promoting a Robust American Bulk Power System

Peter W. Raun[*]

ABSTRACT: The Bulk Power System ("BPS") is one of America's most significant technological and infrastructural achievements. Thanks to the BPS, essentially all Americans have access to electricity that powers homes and businesses 24 hours a day, seven days per week, 365 days per year. While the BPS is an extraordinary achievement, it remains a critical security vulnerability due to its use of antiquated technology. The federal government has worked to regulate public utilities through the implementation of Critical Infrastructure Protection ("CIP") standards, and recently revised its standard related to Cyber Security Incident Reporting and Response Planning (CIP-008-6) to mandate reporting of both actual and attempted Cyber Security Incidents. The recent revisions are a step in the right direction, but critical deficiencies exist in the new version of the standard that will confuse utilities, duplicate reporting efforts, and could deprive utilities of necessary capital to enhance the security posture of their operations. To avoid these consequences, this Note argues that CIP-008-6 should be revised to provide clear direction on what constitutes an "attempted" cyberattack, mandate participation in the Cybersecurity Risk Information Sharing Program, and provide a positive financial incentive for compliance.

[*] J.D. Candidate, The University of Iowa College of Law, 2021; B.S., The University of Nebraska Omaha, 2013.

I. INTRODUCTION

Of the many technologies developed by humankind, none may be as influential in our modern world as electricity. Electricity is responsible for

lighting public spaces, heating and cooling homes, powering essential medical devices, charging a wide variety of personal electronics, and supporting many other functions in modern society. Most Americans today give little or no thought to the electricity that powers their lives—assuming that, with the flip of a switch, the power they need will be available instantly. However, delivering electricity to homes and businesses is a delicate and complex undertaking. Because electric power is difficult to store in bulk, electricity must be generated and used almost instantly.[1] A significant long-term outage thus could have catastrophic effects on the security and prosperity of the United States.

The reliable electricity Americans have come to depend on is made possible by an extraordinary piece of infrastructure: the bulk power system ("BPS"). Colloquially referred to as "the grid,"[2] the bulk power system consists of the generators and transmission lines distributed throughout the lower 48 United States.[3] The BPS is connected to localized distribution networks that are in turn connected to individual homes and businesses.[4] Altogether, the system provides over four trillion kilowatt-hours of electricity per year to Americans in large cities, rural communities, and everywhere in between.[5] The grid itself is "on" 24 hours a day, 7 days per week, 365 days per year and is referred to by some as "the largest machine in the world."[6] The bulk power system is owned by private utilities and regulated by the Federal Energy Regulatory Commission ("FERC"),[7] in one of the most unique public/private partnerships of the modern era.

---

1. Jack Eisenhauer, *Is the Duck Chart Duck Soup? The Challenge of Integrating Renewable Resources into the Grid*, NEXIGHT GRP. (Mar. 4, 2014), https://www.nexightgroup.com/is-the-duck-chart-duck-soup-the-challenge-of-integrating-renewable-resources-into-the-grid [https://perma.cc/AUR3-3KSN].

2. *Electricity Explained: How Electricity Is Delivered to Consumers*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/energyexplained/electricity/delivery-to-consumers.php [https://perma.cc/A7R8-PS6R] (last updated Oct. 22, 2020).

3. OFF. OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, UNITED STATES ELECTRICITY INDUSTRY PRIMER 11 (2015) [hereinafter ELECTRICITY PRIMER], https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf [https://perma.cc/9C82-E2MS]; *see also* 16 U.S.C. § 824*o*(a)(1) (2018) (providing the statutory definition for the bulk power system).

4. *See* W. ELEC. COORDINATING COUNCIL, STATE OF THE INTERCONNECTION (2020), https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/The-Bulk-Power-System.aspx [https://perma.cc/43L3-B59K].

5. Nearly 4.12 trillion kilowatt-hours were generated in the United States in 2019. U.S. ENERGY INFO. ADMIN., SEPTEMBER 2020 MONTHLY ENERGY REVIEW 129 tbl.7.2a (2020), https://www.eia.gov/totalenergy/data/monthly/archive/00352009.pdf [https://perma.cc/3NYF-TSN9].

6. Sonia Aggarwal, *Greasing the Electric Grid, the World's Largest Machine (Op-Ed)*, LIVESCIENCE (Nov. 25, 2014), https://www.livescience.com/48893-improving-efficiency-on-the-electric-grid.html [https://perma.cc/NM46-EGMK].

7. *How the Electricity Grid Works*, UNION OF CONCERNED SCIENTISTS (Feb. 17, 2015), https://www.ucsusa.org/resources/how-electricity-grid-works [https://perma.cc/JPK9-DRYC].

While the American bulk power system is a modern marvel of innovation and infrastructure, it remains more vulnerable than many appreciate. Much of the system was built using what was state-of-the-art technology decades ago, yet much of that technology remains in place today.[8] As the Internet and other technologies have continued to develop, foreign actors have taken advantage of these technologies to write malicious software that can compromise these systems—and their activity is on the rise.[9] Multiple public and private entities have identified the American electric grid as a particularly vulnerable target for foreign malicious cybersecurity activity,[10] and in 2019, utilities in the western United States reported the first known cyberattack on the bulk power system.[11] Utility operators and FERC have taken note of these vulnerabilities and dedicate significant effort to ensuring that the BPS remains secure and reliable. Recently, FERC adopted CIP-008-6—a revised cybersecurity incident response standard—to achieve this goal.[12]

This Note argues that while CIP-008-6 is a step in the right direction to ensure the BPS is more reliable and fault-tolerant, it is deficient in several respects. After exploring the history of the BPS and the various Critical Infrastructure Protection ("CIP") standards meant to protect it, this Note will explain that CIP-008-6's requirement to report attempted cyberattacks is overly broad. In its current state, the regulation's breadth is likely to confuse utility operators and cause them to focus on compliance activities rather than security activities. Furthermore, the current enforcement structure is likely to deprive utilities of capital that could be used to invest in cybersecurity initiatives. This Note will also explain that modifying CIP-008-6 to include more direction concerning what constitutes an "attempt," mandating participation in an existing government cybersecurity monitoring program, and considering changes to the penalty structure for non-complying utilities

8. *See generally* GRETCHEN BAKKE, THE GRID: THE FRAYING WIRES BETWEEN AMERICANS AND OUR ENERGY FUTURE (2016) (discussing the various issues and vulnerabilities of the electric grid due to its age).

9. The first publicly known cyberattack on an electric utility took place in Ukraine in 2015. RICHARD J. CAMPBELL, CONG. RSCH. SERV., ELECTRIC GRID CYBERSECURITY 1 (2018), https://crsreports.congress.gov/product/pdf/R/R45312 [https://perma.cc/PC8S-SW8L].

10. *See* DANIEL R. COATS, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 12 (2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf [https://perma.cc/R4TQ-RBXG] ("New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems." (emphasis omitted)); Anastasios Arampatzis, *Is the Electric Grid Ready to Respond to Increased Cyber Threats?*, TRIPWIRE: STATE SEC. (Oct. 23, 2019), https://www.tripwire.com/state-of-security/ics-security/electric-grid-ready-increased-cyber-threats [https://perma.cc/22CF-P6QU].

11. Blake Sobczak, *Experts Assess Damage After First Cyberattack on U.S. Grid*, E&E NEWS (May 6, 2019), https://www.eenews.net/stories/1060281821 [https://perma.cc/S3GV-U6U2].

12. *FERC Bolsters Cybersecurity for Bulk Electric System*, T&D WORLD (June 26, 2019), https://www.tdworld.com/smart-utility/grid-security/article/20972763/ferc-bolsters-cybersecurity-for-bulk-electric-system [https://perma.cc/3L72-ZHNF].

will likely strengthen CIP-008-6's effectiveness in promoting a robust and secure bulk power system.

II. A BRIEF HISTORY OF CENTRALIZED POWER IN AMERICA

The bulk power system is one of the most complex mechanical systems in the world.[13] While electricity is omnipresent in American life, the finer details of the system's inner workings are unknown to many. The background Section of this Note provides a brief history of the development of the BPS, the key players involved in ensuring the BPS remains operational, and the regulatory framework that governs its continued operation.

A. THE BEGINNINGS OF THE MODERN ENERGY GRID AND EARLY REGULATION OF AMERICAN ENERGY UTILITIES

Centralized electricity distribution has its origins in the late nineteenth century.[14] At first, individuals generated electricity on-site at homes or businesses for personal use.[15] The shift to "centralized" power began in September 1882, when Thomas Edison opened the Pearl Street Station in New York City.[16] General Electric owned the Pearl Street Station, and the facility contained several generators that were connected to nearby "homes and businesses . . . through a network of buried copper wires."[17] The station used Direct Current ("DC") power,[18] which could only be transmitted short distances.[19] Shortly after Edison opened Pearl Street Station, George Westinghouse opened a competing station that transmitted power from

13. Seth Blumsack, *How Complexity Science Can Help Keep the Lights On*, CHRISTIAN SCI. MONITOR (Mar. 2, 2017), https://www.csmonitor.com/Science/Complexity/2017/0302/How-complexity-science-can-help-keep-the-lights-on [https://perma.cc/53CW-BE6A] ("Electric power grids are marvelously complicated and intricate systems, comprising many millions of interconnected turbines, conductors, transmission lines, insulators, switches, and people. They tend to be enormous.").

14. *See History of Electricity*, INST. FOR ENERGY RSCH., https://www.instituteforenergyresearch.org/history-electricity [https://perma.cc/5724-S3K2].

15. *Id.*

16. James E. Hickey, Jr., *Regulation of Electricity Rates in the US: Federal or State Competence?*, 8 J. ENERGY & NAT. RES. L. 105, 107 (1990).

17. *History of Electricity*, *supra* note 14.

18. Robert Peltier, *The Edison of 1879*, POWER MAG. (Aug. 1, 2010), https://www.powermag.com/the-edison-of-1879 [https://perma.cc/D7XX-2W7F].

19. *See* Elizabeth Earley, *Ask an Engineer: What's the Difference Between AC and DC?*, MIT SCH. OF ENG'G (Sept. 17, 2013), https://engineering.mit.edu/engage/ask-an-engineer/whats-the-difference-between-ac-and-dc [https://perma.cc/8UTU-F6N8] (explaining that AC moves further distances than DC power "because the source of the current came from far away, and the wave-like motion of the current makes it an efficient traveler").

Niagara Falls to Buffalo, New York.[20] The Adams Power Plant[21] used Alternating Current ("AC") instead of DC power, which proved to be a significant advantage.[22] AC power became the predominant method of centralized power generation[23] as energy production across America continued to expand. By 1925, "half of all homes in the U.S."[24] enjoyed the benefits of electricity.[25]

While Edison and Westinghouse are responsible for many of electricity's modern developments, Edison's secretary, Samuel Insull, was the true forefather of the modern American energy distribution system.[26] After working for Edison for 11 years,[27] Insull left to join the Chicago Edison Company, a centralized power station, in 1892.[28] In those early days, the equipment used at the plant to generate electricity was extremely expensive to manufacture and install.[29] However, Insull realized that once the plant equipment was in place, expanding delivery to additional homes and businesses (via additional transmission and distribution lines) was an inexpensive method to generate more revenue.[30] He subsequently determined the key to profitable electricity production lay within developing these economies of scale.[31] With this realization in mind, Insull worked aggressively to maximize output, develop a consistent demand for energy,

20. Allison Lantero, *The War of the Currents: AC vs. DC Power*, U.S. DEP'T OF ENERGY (Nov. 18, 2014), https://www.energy.gov/articles/war-currents-ac-vs-dc-power [https://perma.cc/TY9K-6PVQ].

21. Allison C. Meier, *Edward Dean Adams Power Plant*, ATLAS OBSCURA, https://www.atlasobscura.com/places/edward-dean-adams-power-plant [https://perma.cc/78JY-M5NS].

22. Lantero, *supra* note 20.

23. *See id.* ("By this time General Electric had decided to jump on the alternating current train, too.").

24. *The Electric Light System*, NAT'L PARK SERV., https://www.nps.gov/edis/learn/kidsyouth/the-electric-light-system-phonograph-motion-pictures.htm [https://perma.cc/K6QX-XP7H] (last updated Feb. 26, 2015).

25. *Id.*

26. *History of Electricity*, *supra* note 14.

27. *See* Marc Davis, *The Rise and Fall of Samuel Insull*, CHI. TRIB. (Nov. 27, 1994), https://www.chicagotribune.com/news/ct-xpm-1994-11-27-9411270177-story.html [https://perma.cc/KV4P-J4RF] (discussing the career of Insull, including his position as "Edison's private secretary" from 1881 to 1892).

28. Honorable Richard D. Cudahy & William D. Henderson, *From Insull to Enron: Corporate (Re)Regulation After the Rise and Fall of Two Energy Icons*, 26 ENERGY L.J. 35, 41 (2005).

29. *See Public vs. Private Power: From FDR to Today*, FRONTLINE, https://www.pbs.org/wgbh/pages/frontline/shows/blackout/regulation/timeline.html [https://perma.cc/BN5V-EQVZ] (explaining the model under which Insull began to expand his utility business by considering the cost of equipment compared to expansion).

30. *Emergence of Electrical Utilities in America*, SMITHSONIAN INST., https://americanhistory.si.edu/powering/past/h1main.htm [https://perma.cc/AKB5-AY3Q] ("[Insull] also sought new customers, even some rural customers outside the city limits, to help him diversify the company's usage patterns and increase the load factor.").

31. *History of Electricity*, *supra* note 14.

and build larger and more efficient power stations.[32] As his influence in the market grew, Insull also acquired smaller utilities, creating a "natural monopoly"[33] that became the model for energy production.[34]

As electricity continued to increase in popularity across the country, local governments presented two obstacles that threatened to harm the utilities' interests: rate controls and "municipalization."[35] In order to circumvent these issues, utility owners like Insull began to advocate for a new regulatory model that shifted oversight from local to state governments.[36] The model permitted a state regulatory commission to set a maximum rate consumers could be charged for electricity.[37] In return, the commission granted the utility "an exclusive franchise to serve a given geographical area (a legal monopoly)."[38] The case for such a model proved to be persuasive, and by 1914, 43 states had established regulatory commissions to provide oversight.[39]

Against this regulatory backdrop, demand for electricity continued to increase and more utility companies entered the market using Insull's model.[40] Like Chicago Edison, most of these companies controlled every aspect of their individual markets—from generation of electricity to its distribution to customers.[41] As time went on, the successful utility companies began to acquire the smaller utilities at a rapid pace, using "holding companies" to manage their risk in doing so.[42] The rapid rise in holding companies created several large-scale private utility monopolies around the country, and "by the end of the 1920s, ten utility systems controlled [seventy-five percent] of the United States' electric power business."[43]

As America entered the Great Depression, the largest energy utilities in America received heightened scrutiny from Congress and other federal officials.[44] In 1935, despite stiff political opposition, "Congress passed the Public Utility Holding Company Act."[45] The Act mandated the breakup of many of America's largest utility holding companies and required that utilities

32. *Emergence of Electrical Utilities in America*, *supra* note 30.

33. *Id.*

34. *Public vs. Private Power: From FDR to Today*, *supra* note 29.

35. *See History of Electricity*, *supra* note 14. "Municipalization" refers to the possibility that "private investments in electricity infrastructure would be taken over by city or county government." *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Power Grid History*, ITC, https://www.itc-holdings.com/a-modern-power-grid/power-grid-history [https://perma.cc/B2DU-J3VS].

40. *Public vs. Private Power: From FDR to Today*, *supra* note 29.

41. *Id.*

42. *Id.*

43. *Id.*

44. *See Emergence of Electrical Utilities in America*, *supra* note 30.

45. *Public vs. Private Power: From FDR to Today*, *supra* note 2929.

serve only a particular state or region.[46] Less than 25 years after the Act was passed, "the number of [utility] holding companies [in the United States] declined from 216 to 18."[47] This highly regulated structure remained in place until a wave of deregulation began in the late 1970s.[48]

B. INTERCONNECTION AND THE CREATION OF THE MODERN ENERGY GRID

As electricity demand continued to expand throughout America, the need for a larger, more interconnected system became apparent.[49] Power shortages during WWI brought the energy grid's lack of connection into greater focus, and several proposals were developed to make the electricity system in America more robust.[50] The core of these proposals included a concept called "interconnection"—connecting individual electricity networks together—that utility companies initially rejected.[51] However, as growth in the electricity sector increased, interconnection eventually took hold. Today, America's electricity grid consists of three major interconnections: the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas ("ERCOT") Interconnection.[52] The Eastern and Western Interconnections are separated at the Rocky Mountains.[53] While the Interconnections generally operate independently of one another, the Eastern and Western Interconnections themselves are connected by seven different DC tie facilities located in various states throughout the high plains.[54]

Together, the generation systems and transmission lines that supply wholesale electricity to local utilities for distribution are referred to

---

46. *See id.*

47. *Id.*

48. The wave of regulatory change in the utility sector was brought on by the Energy Crisis in the 1970s. *See* Arshak Zakarian, Note, *Competing to Cut Carbon: State Policies, Conflict with Federally-Regulated Energy Markets, and Recommendations*, 15 HASTINGS BUS. L.J. 173, 178 (2019).

49. *See* JOHN L. NEUFELD, SELLING POWER: ECONOMICS, POLICY, AND ELECTRIC UTILITIES BEFORE 1940, at 85 (2016).

50. *Id.*

51. Two different proposals, "Superpower" and "Giant Power," were initially rejected. *Id.* at 85–95. However, characteristics of the "Giant Power" proposal—chiefly, diversified ownership of various aspects of the power system—came back into vogue and can be seen in the structure of today's electricity industry. *See id.* at 90.

52. Sara Hoff, *U.S. Electric System Is Made Up of Interconnections and Balancing Authorities*, U.S. ENERGY INFO. ADMIN. (July 20, 2016), https://www.eia.gov/todayinenergy/detail.php?id=27152 [https://perma.cc/7MLG-UAMY].

53. *Id.*

54. *Energy Education: DC Ties Serve Critical Role in Connecting the Grid*, NMPP ENERGY (July 1, 2018), http://www.nmppenergy.org/mean/news/detail/112-energy-education-dc-ties-serve-critical-role-in-connecting-the-grid [https://perma.cc/F73C-ZT8E]. The DC tie facilities allow a small amount of residual power to be transferred between the two interconnections, "act[ing] as a sort of ultra high-tech 'shock absorber.'" *Id.*

collectively as the "bulk-power system."[55] It comprises over 360,000 miles of transmission lines[56]—enough to circle the Earth over 14 times—and is "on" 24 hours per day, seven days per week, 365 days per year. The challenge of ensuring the grid has sufficient power—but not too much power—is managed by a group of 74 "balancing authorities"—utility operators that handle both generation and distribution of electricity—that receive special authorization to operate the bulk power system.[57] In total, the bulk power system transmitted nearly 4.12 trillion kilowatt-hours ("kWh") of electricity in 2019.[58] As a whole, the electricity infrastructure made possible by the grid has enabled much of the technological progress and modern convenience that Americans enjoy today.

III. THE OVERSEERS OF THE BULK POWER SYSTEM: FERC AND NERC

The bulk power system in America is largely overseen by two organizations—FERC and the North American Electric Reliability Corporation ("NERC").[59] The relationship between FERC and NERC is a unique public/private partnership and is responsible for the standards framework that governs the reliability of the bulk power system.[60] This Section of the Note will briefly explain the formation of the two organizations and how they work together to regulate the BPS.

A. THE CREATION OF THE FEDERAL ENERGY REGULATORY COMMISSION

While Samuel Insull managed to influence states to take action to regulate local power utilities in the early days of power generation, the federal government did not begin addressing power as a matter of public policy until the early 1920s.[61] In 1920, Congress passed the Federal Water Power Act, initially intended to regulate the construction of hydroelectric power projects.[62] As the electricity market continued to grow, the federal government followed the Federal Water Power Act with several other laws and regulations in the following decades, designed to expand power to rural areas and advance the nation's energy infrastructure.[63]

---

55. *See* 16 U.S.C. § 824*o*(a)(1) (2018); Hoff, *supra* note 52.

56. ELECTRICITY PRIMER, *supra* note 3, at 13.

57. Hoff, *supra* note 52.

58. U.S. ENERGY INFO. ADMIN., *supra* note 5, at 129.

59. *See* ELECTRICITY PRIMER, *supra* note 3, at 25.

60. *See id.*

61. WILLIAM F. FOX, JR., FEDERAL REGULATION OF ENERGY 5 (1983) ("Congress was virtually silent on both natural resource policy and environmental protection from 1800 to 1906.").

62. Federal Water Power Act, ch. 285, 41 Stat. 1063 (1920) (codified as amended at 16 U.S.C. § 791 (1921)).

63. *See Public vs. Private Power: From FDR to Today*, *supra* note 29 ("The end result of the New Deal era regulatory intervention into the electric industry led to four primary types of service providers: private investor-owned utilities (IOUs) with stock freely traded in the marketplace by shareholders; publicly owned utilities, such as those owned by municipalities; cooperative utilities

Within the Federal Water Power Act, Congress established the Federal Power Commission.[64] Originally, the Commission was "composed of the Secretary of War, the Secretary of the Interior, and the Secretary of Agriculture"[65] and was charged with inspecting and issuing licenses for the construction and maintenance of hydroelectric dams.[66] The initial structure and membership of the Commission proved to be unworkable,[67] so Congress eventually altered the Commission to consist of five dedicated commissioners.[68] With the passage of the Federal Power Act in 1935, the Federal Power Commission's duties expanded to include "regulatory powers over electric utilities which own or operate facilities for the transmission or sale at wholesale of electric energy in interstate commerce."[69]

The Commission's name and structure remained largely unchanged until 1977, when Congress passed the Department of Energy Organization Act.[70] The Act created the Department of Energy[71] and classified the renamed FERC as an independent agency under the Department.[72]

Today, FERC's mission is to "[a]ssist consumers in obtaining economically efficient, safe, reliable, and secure energy services at a reasonable cost through appropriate regulatory and market means, and collaborative efforts."[73] The Commission still consists of five members, appointed by the President for five-year terms.[74] No more than three members can be from one political party,[75] and the decisions made by the Commission are reviewable by a court, not another political branch of government.[76] A full accounting of FERC's responsibilities vastly exceeds the scope of this Note, but includes the security of the BPS and the sale of electricity as it pertains to

---

which were usually found in rural communities; and federal electric utilities, such as the TVA and REA.").

64. Federal Water Power Act, ch. 285, 41 Stat. at 1063.

65. *Id.*

66. *See* Philip L. Cantelon, *The Regulatory Dilemma of the Federal Power Commission, 1920–1977*, 4 FED. HIST. 61, 62 (2012).

67. Gifford Pinchot, *The Long Struggle for Effective Federal Water Power Legislation*, 14 GEO. WASH. L. REV. 9, 19–20 (1945).

68. *Id.* at 20.

69. Clyde L. Seavey, *Functions of the Federal Power Commission*, 201 ANNALS AM. ACAD. POL. & SOC. SCI. 73, 73 (1939).

70. Department of Energy Organization Act, Pub. L. No. 95-91, 91 Stat. 565 (1977).

71. *Id.* § 201.

72. *Id.* § 204.

73. *About FERC: Overview*, FED. ENERGY REGUL. COMM'N, https://www.ferc.gov/about/what-ferc [https://perma.cc/4TEJ-K36G] (last updated Jan. 21, 2021).

74. 42 U.S.C. § 7171(b)(1) (2018).

75. *Id.*

76. 16 U.S.C. § 825*l*(b) (2018).

"interstate commerce."[77] FERC is specifically prohibited from managing local electricity distribution and sales to individuals.[78]

B. The Creation of the North American Electric Reliability Corporation

While the federal government had created a regulatory body to regulate the interstate aspects of the electricity market, the electricity industry did not begin collectively coordinating its service efforts until the late 1960s.[79] After the Northeast Blackout in 1965, the Federal Power Commission released a report, suggesting the creation of "[a] council on power coordination made up of representatives from each of the nation's Regional coordinating organizations to exchange and disseminate information on Regional coordinating practices to all of the Regional organizations, and to review, discuss, and assist in resolving matters affecting interregional coordination."[80]

In 1968, 12 regional organizations collectively agreed to coordinate operations and signed the agreement that formed the National Electric Reliability Council.[81] Since its formation, NERC's efforts have developed beyond operational coordination to include long-term planning, security implementation, and several other important goals.[82] After adding the Canadian electric grid to the organization, the Council changed its full name to the North American Electric Reliability Council.[83]

Today, NERC is governed by an 11-member board of trustees, consisting of individuals from across the energy sector.[84] NERC supervises the three United States interconnections and the Quebec Interconnection in Canada.[85] Altogether, the organization is responsible for the continued operation of the BPS throughout the lower 48 United States, southern Canada, and a small portion of Mexico.[86] The organization has a budget of approximately $80 million[87] and works to ensure "a highly reliable and secure North American

77. *Id.* § 824.

78. *See id.* § 824(b)(1).

79. DAVID NEVIUS, THE HISTORY OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION 5–6 (2020), https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf [https://perma.cc/L38V-JZ4W].

80. N. AM. ELEC. RELIABILITY CORP., NERC OPERATING MANUAL, at HIST-2 (2016) [hereinafter NERC OPERATING MANUAL], https://www.nerc.com/comm/OC/Operating%20Manual%20DL/Operating_Manual_20160809.pdf [https://perma.cc/2X6A-9U84].

81. NEVIUS, *supra* note 79, at 5.

82. *See* NERC OPERATING MANUAL, *supra* note 80, at 1.

83. *Id.* at HIST-2.

84. N. AM. ELEC. RELIABILITY CORP., BYLAWS 6 (2018), https://www.nerc.com/gov/Annual%20Reports/NERC%20Bylaws_Effective%20September%2025,%202018.pdf [https://perma.cc/5ZPS-Q8V8].

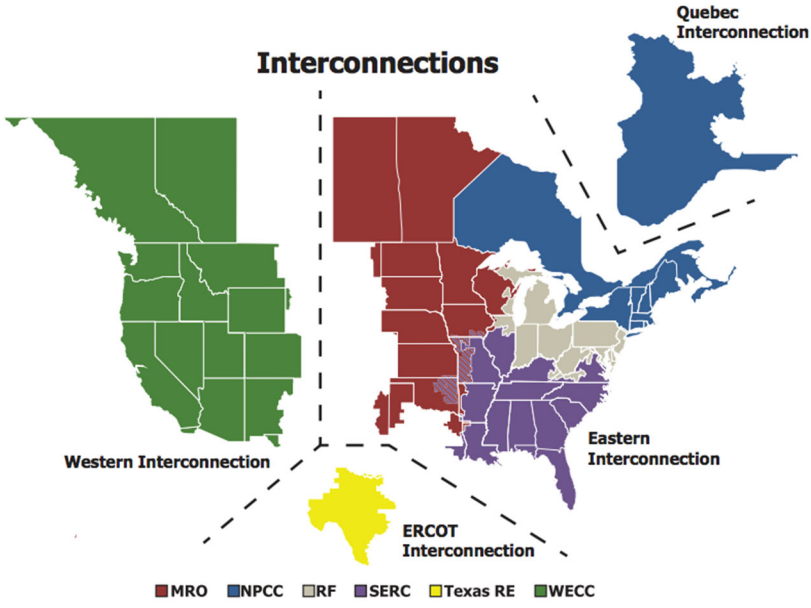
85. ELECTRICITY PRIMER, *supra* note 3, at 25.

86. *Id.*

87. N. AM. ELEC. RELIABILITY CORP., 2020 BUSINESS PLAN AND BUDGET: FINAL 4 (2019), https://www.nerc.com/gov/bot/FINANCE/2020%20NERC%20Business%20Plan%20and%20Bu

bulk power system."[88] NERC partners with entities within the federal government and the private energy sector in order to achieve these goals, and has formed several unique partnerships to ensure compliance with its objectives.[89]

Figure 1. Map of NERC Interconnections[90]



IV. THE RELIABILITY STANDARDS FRAMEWORK FOR THE BULK POWER SYSTEM

In order to facilitate effective oversight, FERC relies on NERC to develop reliability standards for the bulk power system.[91] This Section of the Note will explain the requirement for the reliability standards and how the standards are created and approved. It will then focus on the Critical Infrastructure Protection Standards and CIP-008-6.

---

dget%20DL/NERC%202020%20Business%20Plan%20and%20Budget%20-%20Final.pdf [https://perma.cc/HN88-UFAR].

88. N. AM. ELEC. RELIABILITY CORP. [hereinafter NERC HOMEPAGE], https://www.nerc.com [https://perma.cc/k38e-fs7w].

89. NEVIUS, *supra* note 79, at ix.

90. *NERC Interconnections*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/AboutNERC/keyplayers/PublishingImages/NERC%20Interconnections.pdf [https://perma.cc/WV9D-5JFC].

91. The certified Electric Reliability Organization ("ERO") has the responsibility for developing reliability standards, and NERC has been the nation's ERO since 2006. *See* Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission*, 41 N. KY. L. REV. 437, 440–41 (2014).

A. THE NATIONAL ENERGY POLICY ACT OF 2005 AND STANDARDS DEVELOPMENT PROCESS

FERC and NERC further connected their operations in the early 2000s in the aftermath of the Northeast Blackout of 2003.[92] After the blackout, Congress took action to update several key areas of electricity policy in America.[93] The National Energy Policy Act was passed in 2005 and contained several key amendments to the Federal Power Act to facilitate a more reliable energy grid.[94] Chief among the enhancements was the requirement for the designation of an Electric Reliability Organization ("ERO").[95] The ERO, in turn, is responsible for "develop[ing] and enforc[ing] compliance with reliability standards for only the bulk-power system."[96] FERC designated NERC as the nation's first ERO in 2006,[97] and since then NERC has been responsible for the reliability of the electric grid in the United States.[98]

The standards developed by NERC "define the reliability requirements for planning and operating the North American bulk power system."[99] The standards are developed "using results-based principles that focus on three areas: measurable performance, risk mitigation strategies, and entity capabilities."[100] NERC's comprehensive reliability standards program covers 14 key areas: Resource and Demand Balancing; Critical Infrastructure Protection; Communications; Emergency Preparedness and Operations; Facilities Design, Connections, and Maintenance; Interchange Scheduling and Coordination; Interconnection Reliability Operations and Coordination; Modeling, Data and Analysis; Nuclear; Personnel Performance, Training, and Qualifications; Protection and Control; Transmission Operations; Transmission Planning; and Voltage and Reactive.[101] In addition to reliability

92. The Northeast Blackout of 2003 cut off power to over 50 million people due to sagging power lines that came into contact with trees. *See* Ken Belson & Matthew L. Wald, *'03 Blackout Is Recalled, Amid Lessons Learned*, N.Y. TIMES (Aug. 13, 2008), https://www.nytimes.com/2008/08/14/nyregion/14blackout.html [https://perma.cc/A4FV-3GUP].

93. *Id.*

94. *Id.*

95. 16 U.S.C. § 824*o*(c) (2018).

96. *Id.* § 824*o*(i)(1).

97. Patricia A. Hoffman, *10 Years After the 2003 Northeast Blackout*, U.S. DEP'T OF ENERGY (Aug. 14, 2013), https://www.energy.gov/oe/articles/10-years-after-2003-northeast-blackout [https://perma.cc/V5TC-V793].

98. ELECTRICITY PRIMER, *supra* note 3, at 25.

99. *Standards*, N. AM. ELEC. RELIABILITY CORP. [hereinafter *Standards*, N. AM. ELEC. RELIABILITY CORP.], https://www.nerc.com/pa/Stand/Pages/default.aspx [https://perma.cc/43H6-W64X].

100. *Id.*

101. *See All Reliability Standards*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx [https://perma.cc/C5L4-88M7].

standards related to physical security concerns, NERC enacted a number of cybersecurity regulations in 2008.[102]

All reliability standards are developed in accordance with a structured process overseen by the NERC Standards Committee.[103] The process begins with "[a] Standard Authorization Request."[104] Once the request is completed, the Standards Committee meets to consider the request and its associated documentation.[105] The Committee may then approve the request, remand the request for additional development, delay action on the request, or reject the request.[106] If approved, the proposal is opened for a comment period that lasts for up to 30 days.[107] After the comment period, a drafting team of industry volunteers develops the standard.[108] After a standard is drafted, the Standards Committee facilitates a comment and balloting process, where NERC members may vote and provide feedback on the proposed standard.[109] After the ballot and comment period, the drafting team assesses and responds to the collected comments.[110] Minor changes are made to the standard if needed before conducting a final ballot.[111] Once the standard is approved during the balloting process, it must be adopted by NERC's Board of Trustees.[112] After the Trustees approve of the standard, the documents approved by the Board are submitted to the appropriate governmental authorities (FERC in the United States) for approval.[113]

After approval by FERC, the reliability standards are enforceable by NERC.[114] Adherence to the standards is verified by Regional Entities,[115] who

---

102. *See* Court, *supra* note 91, at 445–46 (describing the eight CIP Reliability Standards that were initially approved by FERC under Order No. 706).

103. *See* N. AM. ELEC. RELIABILITY CORP., APPENDIX 3A: STANDARD PROCESSES MANUAL: VERSION 4, at 7 (2019) [hereinafter NERC STANDARD PROCESSES MANUAL], https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf [https://perma.cc/YS83-5CDX].

104. *See id.* at 13.

105. *See id.*

106. *Id.*

107. *Id.* at 14.

108. *Standards*, N. AM. ELEC. RELIABILITY CORP., *supra* note 99.

109. NERC STANDARD PROCESSES MANUAL, *supra* note 103, at 17–18.

110. *Id.* at 20.

111. *Id.*

112. *Id.* at 21.

113. *Id.*

114. *Id.*

115. There are six Regional Entities, each assigned to cover a different area of North America: the Midwest Reliability Organization ("MRO"), the Northeast Power Coordinating Council, Inc. ("NPCC"), ReliabilityFirst ("RF"), the SERC Reliability Corporation ("SERC"), the Texas Reliability Entity, Inc. ("Texas RE"), and the Western Electricity Coordinating Council ("WECC"). *See Regional Entity Executives*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/AboutNERC/keyplayers/Pages/Regional-Entity-Executives.aspx [https://perma.cc/5Z29-RV8C]; *supra* Figure 1 (providing a map of each Regional Entity's territory).

have the authority to perform compliance monitoring and enforcement activities for utilities in their respective territories.[116] NERC assesses fines and other sanctions against operators who violate these standards.[117] When a potential violation is discovered or reported, a "Notice of Possible Violation" is issued to the utility and an investigation is conducted by a Regional Entity.[118] If the investigation reveals a standards violation, the Regional Entity will issue a notification of an alleged violation, along with a proposed penalty determined using NERC's Sanction Guidelines.[119] The Sanction Guidelines set by NERC include detailed instructions pertaining to the calculation of fines or other sanctions in accordance with the standard's Violation Risk Factor[120] and Violation Severity Level.[121] Once the notice is received, the utility may accept the violation, contest the violation, or opt for a settlement with NERC.[122]

B. THE FIRST CRITICAL INFRASTRUCTURE PROTECTION ("CIP") STANDARDS

NERC began promulgating its first mandatory cybersecurity standards for the bulk power system shortly after being designated as the Electric Reliability Organization for the United States.[123] NERC formally proposed the first round of Critical Infrastructure Protection ("CIP") standards on August 28, 2006.[124] Designed to "provide a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks," the new mandatory

116. *Compliance Assurance*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/comp/Pages/AboutComplianceOperations.aspx [https://perma.cc/U3QV-G2B4].

117. *Compliance & Enforcement*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/comp/Pages/default.aspx [https://perma.cc/7R32-RVYM].

118. N. AM. ELEC. RELIABILITY CORP., COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM: APPENDIX 4C TO THE RULES OF PROCEDURE §§ 5.1–5.2 (2018) [hereinafter NERC COMPLIANCE MONITORING & ENFORCEMENT PROGRAM], https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_06082018.pdf [https://perma.cc/LTP6-2VHB].

119. *Id.* § 5.3.

120. Violation Risk Factors "are assigned . . . to provide clear, concise and comparative association[s] between the violation of a Requirement and the expected or potential impact of the violation to the reliability of the Bulk Power System." N. AM. ELEC. RELIABILITY CORP., SANCTION GUIDELINES OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION: APPENDIX 4B § 3.1.1 (2014) [hereinafter NERC SANCTION GUIDELINES], https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4B_SanctionGuidelines_20140701.pdf [https://perma.cc/F4LY-DZA3].

121. Violation Severity Levels "are defined levels of the degree to which a Requirement of a Reliability Standard was violated." *Id.* § 3.1.2.

122. NERC COMPLIANCE MONITORING & ENFORCEMENT PROGRAM, *supra* note 118, §§ 5.4, 5.6. The fines assessed by NERC can be significant. In 2019, NERC levied one of its largest fines ever recorded—$10 million from a single utility. *See* Brandon Workentin, *Largest NERC CIP Fine to Date: What You Need to Know*, FORESCOUT (Feb. 1, 2019), https://www.forescout.com/company/blog/largest-nerc-cip-fine-to-date [https://perma.cc/Y3BM-KT8A].

123. Mandatory Reliability Standards for Critical Infrastructure Protection, 73 Fed. Reg. 7368, 7369 (Feb. 7, 2008) (to be codified at 18 C.F.R. pt. 40).

124. *Id.*

standards replaced a voluntary cybersecurity standard initially adopted in 2003.[125] In total, NERC proposed eight different standards in its first round, relating to security management controls, physical and electronic perimeter security, incident reporting and response planning, and recovery plans.[126] In addition to the eight standards, "NERC submitted 162 Violation Risk Factors that correspond to Requirements of the proposed CIP Reliability Standards."[127] The Violation Risk Factors "are used by NERC and the Regional Entities to determine financial penalties for violating a Reliability Standard."[128] Third, NERC proposed an implementation timeline for the new standards "that provides for a three-year phase-in to achieve full compliance with all requirements."[129]

Nearly two years later, on January 18, 2008, FERC approved the reliability standards via Order No. 706.[130] In approving the standards, the Commission determined the standards were "just and reasonable, not unduly discriminatory or preferential and in the public interest."[131] While under FERC consideration, the regulations enjoyed generally broad support from the public.[132]

C. THE FORMER STANDARD: CIP-008-5

The CIP standard under contemplation in this Note is CIP-008: Incident Reporting and Response Planning. NERC initially included CIP-008 in the initial suite of its proposed Reliability Standards in 2006.[133] Since being initially adopted with the other CIP standards in Order No. 706, CIP-008 has undergone a series of revisions.[134] FERC enacted the latest version, CIP-008-5, in November 2013.[135] CIP-008-5's stated purpose is "[t]o mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements."[136] The standard is applicable to

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.* at 7368.

131. *Id.* at 7370.

132. *Id.* ("Most commenters strongly support the Commission's proposal to approve the CIP Reliability Standards as mandatory and enforceable.").

133. *Id.* at 7369.

134. *Id.*

135. Critical Infrastructure Protection Reliability Standards, 78 Fed. Reg. 72,756, 72,756 (Dec. 3, 2013) (to be codified at 18 C.F.R. pt. 40).

136. N. AM. ELEC. RELIABILITY CORP., CIP-008-5—CYBER SECURITY—INCIDENT REPORTING AND RESPONSE PLANNING 1 (2016) [hereinafter CIP-008-5], https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-008-5&title=Cyber%20Security%20-%20Incident%20Reporting%20and%20Response%20Planning&jurisdiction=United%20States [https://perma.cc/28QZ-7XEW].

all "Responsible Entities," which include balancing authorities, distribution providers, generator operators and owners, interchange coordinators or authorities, reliability coordinators, and transmission operators and owners.[137]

Under the standard, each "Responsible Entity"[138] must create a Cyber Security Incident Response Plan.[139] The plans must contain three general elements: (1) Specifications; (2) Implementation and Testing; and (3) Review, Update, and Communication.[140] Under the first element, entities must create specifications including "[o]ne or more processes to identify, classify, and respond to Cyber Security Incidents."[141] The plan must also specify a process to determine whether the Incident is of sufficient magnitude to be a "Reportable Cyber Security Incident[]" that must be reported to the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC") within one hour of its determination.[142] The plan must also specify "roles and responsibilities"[143] of those involved in resolving the Incident and "[i]ncident handling procedures for Cyber Security Incidents."[144] The second element requires that the Cyber Security Incident Response Plan(s) be tested "at least once every 15 calendar months"[145] and that all records related to the Incidents and tests be retained.[146] Finally, after the plan has been developed and implemented or tested, the Responsible Entity must "[d]ocument any lessons learned or . . . the absence of any lessons learned"[147] and update the plan as necessary.[148] The plan must also be updated if roles or responsibilities change

137. *Id.* at 1–2.

138. Within the NERC standards framework, "Responsible Entities" refers to the collective list of entities to whom the standard applies.

139. CIP-008-5, *supra* note 136, at 5.

140. *See id.* at 5–11 (enumerating the requirements for a Cyber Security Incident Response Plan development in a series of tables that include criteria for Specifications, Implementation/Testing, and Review/Update/Communication).

141. *Id.* at 5 tbl.R1.

142. *Id.* at 19 ("The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable . . . ."). ES-ISAC was renamed and is now called the Electricity Information Sharing and Analysis Center ("E-ISAC"). Nick Santora, *ES-ISAC is Now E-ISAC*, CURRICULA (Nov. 18, 2015), https://www.getcurricula.com/es-isac-now-e-isac [https://perma.cc/44ZB-ADBF]. The entity is referred to as "E-ISAC" elsewhere in this Note.

143. CIP-008-5, *supra* note 136, at 6.

144. *Id.*

145. *Id.* at 7 tbl.R2.

146. *Id.* at 8. Entities are required to keep data under the CIP-008 standard for three calendar years, and "[i]f a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer." *Id.* at 12.

147. *Id.* at 10.

148. *Id.*

in any significant fashion.[149] To support these requirements, the standard identifies particular types of evidence that may be used to support the creation and maintenance of the Cyber Security Incident Response Plan.[150] All three required elements carry Violation Risk Factors of "Lower" for the purposes of assessing penalties under the Sanction Guidelines.[151]

D. THE NEW STANDARD: CIP-008-6

NERC developed the latest iteration of CIP-008 in response to FERC Order No. 848.[152] In the July 2018 order, FERC "observed that Cyber Security Incidents are presently reported by responsible entities in accordance with . . . CIP-008-5."[153] However, the Commission expressed a concern "that the current reporting threshold may understate the true scope of cyber-related threats facing the Bulk-Power System, particularly given the lack of any reportable incidents in 2015 and 2016."[154] To increase the amount of submitted reports, FERC requested that "NERC . . . develop and submit modifications to the NERC Reliability Standards to augment current mandatory reporting of Cyber Security Incidents, *including incidents that might facilitate subsequent efforts to harm the reliable operation of the* [*bulk electric system*]."[155]

In its order, FERC directed NERC to provide for the following four elements in its new standard.[156] First, all entities subject to the requirements of CIP-008 "must report Cyber Security Incidents that compromise, *or attempt to compromise*, a responsible entity's ESP[157] or associated EACMS."[158] Second, a minimum amount of requisite information from the entities should be

149. *Id.* at 11. Entities have 60 calendar days to update plans and notify individuals "with a defined role in the Cyber Security Incident response plan of the updates." *Id.*

150. *Id.*

151. *Id.* at 5, 7, 9.

152. Cyber Security Incident Reporting Reliability Standards, 83 Fed. Reg. 36,727, 36,727 (July 31, 2018) (to be codified at 18 C.F.R. pt. 40).

153. *Id.* at 36,728.

154. *Id.*

155. *Id.* at 36,730 (emphasis added).

156. *Id.* at 36,728.

157. Electronic Security Perimeter. *See* N. AM. ELEC. RELIABILITY CORP., CIP-005-5—CYBER SECURITY—ELECTRONIC SECURITY PERIMETER(S) 16 (2012), https://www.nerc.com/pa/Stand/ReliabilityStandards/Reliability%20Standards%20DL/CIP-005-5.pdf [https://perma.cc/LV93-CNQR] ("The Electronic Security Perimeter ('ESP') serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.").

158. Cyber Security Incident Reporting Reliability Standards, 83 Fed. Reg. at 36,728 (emphasis added). "EACMS" refers to "Electronic Access Control or Monitoring Systems" and consists of "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems." N. AM. ELEC. RELIABILITY CORP., GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS (2021), https://www.nerc.com/files/glossary_of_terms.pdf [https://perma.cc/XK3G-LRHP].

included in each report "to improve the quality of reporting and allow for ease of comparison."[159] Specifically, the Commission requested that entities report an incident's "functional impact," "attack vector," and "level of intrusion achieved or attempted by the Cyber Security Incident."[160] Third, FERC directed NERC to develop specific timetables for entities to follow when reporting an incident or attempt.[161] Fourth, reports of Cyber Security Incidents, in addition to being sent to E-ISAC, "should . . . be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS–CERT)."[162] In addition to the specific reports, NERC was directed to create and share "an annual, public, and anonymized summary of the reports with the Commission."[163] FERC also requested that the new standard be implemented quickly, setting a deadline of April 1, 2019—less than a year after the original order was filed.[164]

In response to FERC's order, NERC began working to update the provisions of CIP-008-5 on August 6, 2018.[165] The Standards Committee released an initial draft of the revised standard two months later.[166] The draft contained several changes to the existing three requirements of CIP-008-5 and an additional requirement to facilitate reporting the incidents to E-ISAC and to the Department of Homeland Security.[167] Additionally, NERC

159. Cyber Security Incident Reporting Reliability Standards, 83 Fed. Reg. at 36,728.

160. *Id.* at 36,730.

161. *Id.* at 36,728.

162. *Id.*

163. *Id.*

164. *See* N. AM. ELEC. RELIABILITY CORP., CIP-008-6: PROJECT 2018-02 MODIFICATIONS TO CIP-008 CYBER SECURITY INCIDENT REPORTING: CONSIDERATION OF COMMENTS 12 (2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Consideration_of_Comments_Final%20Ballot_01152019.pdf [https://perma.cc/K2FU-KUF2] ("[T]he standard drafting process requires NERC Board of Trustee approval before filing with FERC to meet [the] order 848 deadline of April 1, 2019.").

165. N. AM. ELEC. RELIABILITY CORP., STANDARD AUTHORIZATION REQUEST (SAR): REVISIONS TO CIP-008-5 CYBER SECURITY—INCIDENT REPORTING AND RESPONSE PLANNING 1 (2018), https://www.nerc.com/pa/Stand/Project%201802%20Modifications%20to%20CIP008%20Cyber%20Secur/2018-02_CIP-008_Standard_Authorization_Request_08102018.pdf [https://perma.cc/5J3Y-K4R6].

166. *See* N. AM. ELEC. RELIABILITY CORP., STANDARDS ANNOUNCEMENT: PROJECT 2018-02 MODIFICATIONS TO CIP-008 CYBER SECURITY INCIDENT REPORTING 1 (2018) [hereinafter CIP-008-6 OCTOBER STANDARDS ANNOUNCEMENT], https://www.nerc.com/pa/Stand/Project%201802%20Modifications%20to%20CIP008%20Cyber%20Secur/2018-02_CIP-008-6_CP_BP_IB_NBP_Word_Announce_10032018.pdf [https://perma.cc/3GP6-PFBX].

167. N. AM. ELEC. RELIABILITY CORP., CIP-008-6—CYBER SECURITY—INCIDENT REPORTING AND RESPONSE PLANNING 17 (2018), https://www.nerc.com/pa/Stand/Project%201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Standard_Redline_10032018.pdf [https://perma.cc/5B5M-QZUM] ("Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and each United States Responsible Entity also shall notify the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), or their successors, of Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents . . . .").

included an implementation plan, explaining how the standard would be implemented, along with a proposed timeline.[168] However, conspicuously absent from the plan was a clear definition for what constitutes "a Reportable Attempted Cyber Security Incident."[169]

After the standard was drafted, NERC opened the standard to a 20-day comment period, followed by an initial ballot of NERC members.[170] During the comment process, several members commented that the definition of "attempt" was overly broad.[171] NERC responded to the concerns, stating:

> [I]t is to the industry's benefit that CIP-008 leaves it up to each Responsible Entity to document a process to determine what constitutes an "attempt". The SDT further asserts that no two Responsible Entities are alike and the determination of "attempts" is contextual and dependent on what is normal within each unique organization. To define "attempt" could create an overly prescriptive and less risk-based approach and may have the unintended consequence of undue administrative burden or removal of needed discretion and professional judgment from subject matter experts.[172]

In accordance with its established standards development process, NERC facilitated a preliminary ballot on the CIP-008 revision.[173] At the preliminary

168. *See generally* N. AM. ELEC. RELIABILITY CORP., IMPLEMENTATION PLAN: PROJECT 2018-02 MODIFICATIONS TO CIP-008 CYBER SECURITY INCIDENT REPORTING | RELIABILITY STANDARD CIP-008-6 (2018) [hereinafter CIP-008-6 IMPLEMENTATION PLAN], https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/2018-02_CIP-008-Implementation%20Plan_10032018.pdf [https://perma.cc/LFU2-5SS4] (detailing the plan for Responsible Entities to implement CIP-008-6).

169. The absence of a standard definition of "attempt" was noted by many Responsible Entities, particularly during the first comment period. *See* N. AM. ELEC. RELIABILITY CORP., CIP-008-6: PROJECT 2018-02 MODIFICATIONS TO CIP-008 CYBER SECURITY INCIDENT REPORTING: CONSIDERATION OF COMMENTS 7 (2018) [hereinafter CIP-008-6 NOVEMBER CONSIDERATION OF COMMENTS], https://www.nerc.com/pa/Stand/Project%201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008-6_Consideration_of_Comments_Draft_11152018.pdf [https://perma.cc/2QM8-ATP4] ("Several commenters expressed concern about the determination of 'attempts' and requested the SDT either define 'attempts' or provide clear examples within Implementation Guidance to aid the industry.").

170. CIP-008-6 OCTOBER STANDARDS ANNOUNCEMENT, *supra* note 166, at 1.

171. *See generally* N. AM. ELEC. RELIABILITY CORP., COMMENT REPORT: 2018-02 MODIFICATIONS TO CIP-008 CYBER SECURITY INCIDENT REPORTING | CIP-008-6 (2018), https://www.nerc.com/pa/Stand/Project%201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008_Comments_Received_10222018.pdf [https://perma.cc/7NQ6-DNVS] (containing a number of comments that indicate the utilities are dissatisfied with the lack of definition for "attempt" in the new standard).

172. CIP-008-6 NOVEMBER CONSIDERATION OF COMMENTS, *supra* note 169, at 8.

173. CIP-008-6 OCTOBER STANDARDS ANNOUNCEMENT, *supra* note 166, at 1.

ballot stage, the regulation failed to win the support of NERC membership by a vote of 54–201.[174]

While NERC made several adjustments to the proposed standard prior to its passage, the revisions did not include an expanded definition of "attempt."[175] NERC facilitated a second round of commenting and balloting before the final regulation was proposed on January 15, 2019. NERC membership ultimately approved the final draft of the regulation by a margin of 238–60. NERC's Board of Trustees approved the newest version of CIP-008 on February 7, 2019. FERC approved the standard on June 20, 2019, and CIP-008-6 became effective and enforceable beginning January 1, 2021.[176]

V. CIP-008-6 IS A STEP IN THE RIGHT DIRECTION, BUT KEY DEFICIENCIES EXIST

The modifications implemented in CIP-008-6 are a step in the right direction; however, the standard remains deficient in several respects. Requiring additional reporting of attempts will likely lead to a larger body of cybersecurity knowledge, which will benefit the utilities and the government in the long term. However, key deficiencies exist that may limit the standard's effectiveness. First, without a uniform definition of "attempt," the standard is exceedingly flexible and potentially open to abuse. Second, requiring each utility to report attempted cybersecurity incidents may cause the utilities to focus on compliance activities, rather than security activities. Finally, requiring utilities to pay a monetary penalty for a small violation may negatively impact a utility's ability to finance cybersecurity enhancements.

A. THE DEFINITION OF "ATTEMPT" IS OVERLY BROAD AND LEAVES THE STANDARD OPEN TO POTENTIAL ABUSE

First, NERC's reluctance to formally define "attempt" creates a flexible standard that is open to potential abuse. Utilities may find it challenging to implement the new standard's vague wording. NERC's inability to sufficiently specify the requirements of potential regulations has already posed problems for their operations.[177] As a Government Accountability Office ("GAO")

174. *Ballot Results: 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 IN 1 ST*, NERC BALLOTING TOOL, https://sbs.nerc.net/BallotResults/Index/305 [https://perma.cc/6SHB-2KFZ].

175. *See generally* CIP-008-6 IMPLEMENTATION PLAN, *supra* note 168 (demonstrating that a definition for "attempt" was not provided in the standard).

176. *See id.* at 2 ("Where approval by an applicable governmental authority is required, *the standard shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the applicable governmental authority's order approving the standard*, or as otherwise provided for by the applicable governmental authority." (emphasis added)).

177. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-332, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT CYBERSECURITY RISKS FACING THE ELECTRIC GRID 34 (2019) [hereinafter GAO-19-332], https://energycommerce.house.gov/

report notes: "[O]ne asset owner explained that FERC-approved cybersecurity standards do not always include details that are needed to understand how they apply to that owner's environment."[178] Because the standards do not include sufficient implementation details, "significant time and effort is required to understand the standards and how they might be implemented."[179] Such standards are burdensome for utilities to implement, and without sufficient clarity, some utilities may inadvertently fail to comply or purposefully take advantage of the standard's vagueness to avoid compliance. Crafting a sufficiently specific definition of "attempt" will assist utilities in understanding what must be done to implement and comply with the standard, which will benefit the government in its goal to acquire new information about cyberattacks.

B. THE BROADENING OF CIP-008-6 MAY PUSH UTILITIES TO CHOOSE COMPLIANCE ACTIVITIES OVER SECURITY ACTIVITIES

Additionally, broadening the regulation to require the reporting of all cybersecurity breach attempts, without providing an appropriate definition, could shift utilities' focuses to compliance activities rather than security activities. On average, a single computer with Internet access experiences over 2,000 cyberattacks *in a single day*.[180] If a report must be filed each time an attempted cyberattack is discovered, hundreds of "attempts" could be reported every hour, even if the utility experiences no adverse functional impact. The reports of these harmless attempts could be time-consuming for each utility to provide and may distract utilities from truly significant security issues. Furthermore, if fines are levied against the utilities for failure to report these attempts,[181] the regulation may have the effect of encouraging utilities to focus on compliance activities,[182] rather than on actually securing their cyber assets—the entire point of the regulation in the first place.[183]

---

sites/democrats.energycommerce.house.gov/files/documents/GAO%20Cybersecurity%20Grid%20Report%202019.pdf [https://perma.cc/M54M-5ZCR].

178. *Id.*

179. *Id.*

180. This is likely a conservative estimate, as the latest available statistic was published in 2007. *Study: Hackers Attack Every 39 Seconds*, A. JAMES CLARK SCH. OF ENG'G (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds [https://perma.cc/T3JZ-D3WH] (noting that the computers in the study were hacked over 2,200 times per day). Furthermore, malicious actors have already successfully targeted the American bulk power system. *See supra* text accompanying note 11.

181. The violation risk factors associated with CIP-008-6 could net fines of anywhere between $1,000 and $25,000 per day. *See infra* note 184 and accompanying text.

182. *See* Sonal Patel, *FERC Mandates Reporting of Attempted Cybersecurity Breaches*, POWER MAG. (July 19, 2018), https://www.powermag.com/ferc-mandates-reporting-of-attempted-cybersecurity-breaches/ [https://perma.cc/JU9C-GDG4] (noting that several electricity industry trade organizations consider CIP-008-6's new requirements to be duplicative and burdensome).

183. *Id.*

C. *Requiring Utilities to Pay a Monetary Fine for Violating the Standard Will Prevent Utilities from Investing Additional Funds on Security Enhancements*

Finally, assessing monetary fines for failing to report an attempted cybersecurity attack may not be the most effective method to increase the security of the BPS. At present under the broadened standard, if a utility does not comply with CIP-008, the utility will be forced to arbitrate the issue with NERC and potentially face a steep fine in the process.[184] While it is unlikely that a utility will be fined for not complying with CIP-008 alone,[185] any fine the utilities are required to pay will necessarily require the utility to use funds that could otherwise be spent to update its aging technology in a meaningful way. It may not be prudent for NERC to impose fines on the offending utility. Instead, NERC should compel utilities to spend their money in a way that more appropriately reflects the spirit of the standard: updating technology so that BPS cyberattacks do not happen in the first place. These issues, taken together, illustrate some of the more problematic aspects of CIP-008-6 and NERC's approach to rectifying cybersecurity issues.

VI. Three Proposed Solutions to Strengthen CIP-008-6

While CIP-008-6 is admittedly imperfect, the regulation could be improved in a number of ways. First, the regulation could be updated to provide more direction to utilities attempting to prudently identify and classify attempted cyberattacks. Second, CIP-008-6 could require BPS operators to participate in an existing program designed to proactively identify attempted and actual cybersecurity attacks. Third, NERC could consider creating a positive financial incentive for compliance with CIP-008-6 that would promote additional investment in cybersecurity technology.

---

184. *See generally* NERC Sanction Guidelines, *supra* note 120 (detailing the process for determining penalties for violations). Because the Violation Risk Factors for CIP-008-6's requirements are classified as "[l]ower," the new requirements added to CIP-008-6 could allow NERC or a regional entity to charge up to $25,000 per day for noncompliance with the standard, depending upon the severity level of the violation. *Id.* at 14. *See also generally* N. Am. Elec. Reliability Corp., Violation Risk Factor and Violation Severity Level Justification: Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting (2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP-008_VRF_VSL_Justifications_R1_R4_Final%20Ballot_Clean_01152019.pdf [https://perma.cc/T5T5-SU9B] (outlining the various violation risk factor and violation severity level justifications that apply to CIP-008, which determine the amount an entity may be fined for a violation).

185. CIP-008 violations that have resulted in fines generally have been coupled with violations of other CIP standards. *See* N. Am. Elec. Reliability Corp., Searchable Notice of Penalty (NOP) Spreadsheet (2019), https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Searchable_Enforcement_Page_09262019.xlsx [https://perma.cc/X5T4-2FG2].

A. CIP-008-6 CAN PROVIDE ADDITIONAL DIRECTION ON "ATTEMPTED" CYBERSECURITY ATTACKS

First, CIP-008-6 could be updated to provide more guidance to utilities attempting to prudently identify and classify attempted cyberattacks. The federal government has a number of resources to help both public and private organizations appropriately classify attempted cyberattacks through the National Institute of Standards and Technology ("NIST") standards.[186] Several organizations, both public and private, have successfully customized the NIST framework to meet their individual needs.[187] Information from these standards could be customized slightly by NERC to apply to utilities' more specific cybersecurity needs. The information could then be distributed as guidance to accompany the regulation[188] or be incorporated into CIP-008 directly.

On the other hand, creating a uniformly implementable cybersecurity standard could introduce risk by creating a larger target for a malicious actor.[189] A diversity in technologies can, in itself, serve as a strength.[190] If the

186. *Cybersecurity Framework: New to Framework*, NAT'L INST. OF STANDARDS & TECH. (Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework [https://perma.cc/CL7Z-XWXV] ("Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.").

187. Joseph Perry, *Explaining the Breakout Success of the NIST Cybersecurity Framework*, INFOSECURITY MAG. (Apr. 16, 2019), https://www.infosecurity-magazine.com/opinions/breakout-nist-cybersecurity-1-1 [https://perma.cc/Q75Q-XXKG] ("In the handful of years since the NIST Cybersecurity Framework . . . was developed, it's been widely modeled in the US and by many other countries and organizations internationally. In fact, it's been so successful in creating common standards around cybersecurity that people sometimes forget the CSF is a voluntary mechanism, not a regulation.").

188. NERC has put forth some effort to help entities understand how to implement the standard, and have even recommended that utilities consider the NIST framework in order to devise their response plans. *See* N. AM. ELEC. RELIABILITY CORP., CYBER SECURITY—INCIDENT REPORTING AND RESPONSE PLANNING: IMPLEMENTATION GUIDANCE FOR CIP-008-6, at 26–27, 36 (2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/Implementation_Guidance_for_CIP-008-6_Final_Ballot_01152019.pdf [https://perma.cc/THR7-PJ33]. However, NERC's guidance still requires the Registered Entities to define "attempts to compromise" for themselves. *See id.* at 20. Because CIP-008-6 does not include a firm definition for "attempt to compromise," it is unclear whether a utility would be penalized for inadvertently or purposefully failing to follow the guidance in crafting their own definition of the term (and thus, what is reported).

189. *See* Jaynarayan H. Lala & Fred B. Schneider, *IT Monoculture: Security Risks and Defenses*, IEEE SEC. & PRIV., Jan./Feb. 2009, at 12, 12 ("[T]he computers comprising an IT monoculture will, by definition, share vulnerabilities, which puts the entire networked system at risk of a rapidly spreading virus or other malware vector.").

190. BENJAMIN COX ET AL., N-VARIANT SYSTEMS: A SECRETLESS FRAMEWORK FOR SECURITY THROUGH DIVERSITY 105 (2006), http://static.usenix.org/event/seco6/tech/full_papers/cox/cox.pdf [https://perma.cc/LA2C-RL4A] ("Many security researchers have noted that the current computing monoculture leaves our infrastructure vulnerable to a massive, rapid attack.

technologies employed are not uniform, but equally secure, a malicious actor will be unable to apply identical techniques to access multiple systems.[191] The inability to use the same technique will slow an attempt to infiltrate multiple systems at once, making a large-scale attack difficult to complete successfully.[192] Because not all systems are designed the same, NERC's argument that "a one-size-fits-all approach"[193] would be functionally sub-optimal is at least credible.[194]

B. CIP-008-6 CAN MANDATE PARTICIPATION IN THE CYBERSECURITY RISK INFORMATION SHARING PROGRAM

In addition, the government has previously worked with utilities to proactively identify cybersecurity issues on a voluntary basis.[195] The most significant embodiment of these efforts is the Cybersecurity Risk Information Sharing Program ("CRISP").[196] While currently a voluntary program, CRISP innovatively works to identify sources of cyberattacks and report them to management to ensure the threat is neutralized.[197] The program is facilitated "in near-real time by installing an information sharing device (ISD) at the border of their information technology (IT) systems."[198] The device then shares information with both the Department of Energy and one of the National Laboratories for analysis.[199] Once the data is analyzed, it is shared with the utility owners/operators via E-ISAC.[200] The program facilitates analysis of both classified and unclassified information, depending on the

One mitigation strategy that has been proposed is to increase software diversity." (citations omitted)).

191. *See id.*

192. Per Larsen, Stefan Brunthaler & Michael Franz, *Security Through Diversity: Are We There Yet?*, IEEE SEC. & PRIV., Mar./Apr. 2014, at 28, 28 ("[S]oftware diversity makes the software running on each individual system unique—and different from that of the attacker.").

193. *See* Petition of North American Electric Reliability Corporation (NERC) for Approval of Proposed Reliability Standard CIP-008-6—Cyber Security—Incident Reporting and Response Planning, 84 Fed. Reg. 30,105, 30,106 (June 26, 2019).

194. *However, allowing utilities and grid operators to implement standards after their own fashion* can create serious problems. The blackouts experienced in Texas in February 2021 are one such example—and attributable, in part, to ERCOT's lax approach to implementing regulations. *See* Will Englund, Steven Mufson & Dino Grandoni, *Texas, the Go-It-Alone State, Is Rattled by the Failure to Keep the Lights On*, WASH. POST (Feb. 18, 2021, 3:34 PM), https://www.washingtonpost.com/business/2021/02/18/texas-electric-grid-failure [https://perma.cc/3U9V-PQ6M].

195. GAO-19-332, *supra* note 177, at 36.

196. U.S. DEP'T OF ENERGY, CYBERSECURITY RISK INFORMATION SHARING PROGRAM (CRISP) 1 (2018), https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf [https://perma.cc/Z9CK-3DU5].

197. GAO 19-332, *supra* note 177, at 36.

198. U.S. DEP'T OF ENERGY, *supra* note 196, at 1.

199. *Id.*

200. *Id.*

nature of the intrusion and analysis taking place.[201] The program is voluntary and has been managed by E-ISAC for several years.[202]

CRISP has generally been met with enthusiasm by the private utility companies and appears to be a success thus far.[203] However, nearly a quarter of energy utilities have not yet begun participating in CRISP.[204] Fortunately, a fix is obvious: NERC should revise CIP-oo8-6 to mandate participation in CRISP. The balancing authorities are uniquely situated to coordinate the installation of the required hardware for participation in the program. Furthermore, because E-ISAC is under NERC's jurisdictional umbrella,[205] NERC would be well-positioned to ensure that CRISP is effectively administered.

Using CRISP to proactively detect cyberthreats would benefit both regulators and utilities alike. Allowing network traffic to be proactively shared with DOE's analysts would facilitate a more robust and swift data analysis by an independent entity. This approach is particularly beneficial to government regulators because they would have an opportunity to analyze the data firsthand as it is generated. The government can be confident it is working with a complete and available set of data and can properly analyze cybersecurity threats and attempts. Participation in CRISP would also ensure that E-ISAC is involved from the start of any perceived attack, allowing for the best possible response to be appropriately formulated. Allowing the regulator to perform most of the analysis would further ensure that issues are analyzed impartially and violations are assessed equally.

Required participation in CRISP would also benefit utility companies by allowing them to offset some costs of information technology analysis onto the government. Information security technology analysis is complex, expensive, time-consuming, and amorphous in many respects.[206] While many utilities may not be well-suited for such a task without significant expense, the size and specialization of the United States' intelligence apparatus is likely to

---

201. *Id.* at 1–2.

202. *Id.*

203. *Id.* at 1 ("Electric utilities participating in the program now account for about 75% of U.S. electric customers.").

204. *See id.*

205. *Electricity Information Sharing and Analysis Center*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx [https://perma.cc/DFL8-HSWZ] ("[T]he E-ISAC is operated by NERC [but] is organizationally isolated from NERC's enforcement processes.").

206. The unwieldy nature of managing information security threats is increasingly expensive—the amount of capital spent annually on information technology security has increased greatly as technology has continued to evolve. *See* Susan Moore & Emma Keen, *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*, GARTNER (Aug. 15, 2018), https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 [https://perma.cc/2SKU-4SZX].

be better suited for such a challenge. Participation in CRISP will allow utilities to avoid a significant expenditure in technology and human resources while largely achieving the goal of enhanced reporting of cybersecurity issues. While it is likely utilities will still have to make at least some investment in their own cybersecurity initiatives, participating in CRISP could be much less expensive compared to the cost of maintaining an independent apparatus for information security analysis or engaging a vendor to do so.

C. CIP-008-6 Can Provide a Positive Financial Incentive for Compliance

Furthermore, FERC and NERC could re-evaluate the penalty structure applied to utilities for noncompliance with its standards. NERC's current system of fines and enforcement certainly provides an incentive for utilities to comply with the regulations in place. However, it also necessarily deprives utilities of capital that could be used to implement new systems with enhanced security features to protect against cyberattacks. While a penalty may be appropriate to promote adherence to the standards, occasionally, a utility's ability to pay the cost of complying with the standard in addition to the fine may be hampered by the size of the fine levied against it. A fine structure that is more sensitive to this reality may be of benefit to the utility's cybersecurity posture.

From a policy perspective, a revised penalty structure for lower risk violations in the Sanction Guidelines that focuses on enhancing the cybersecurity posture of the utility operators, rather than punishing them for noncompliance, may be more effective. One such approach may involve NERC setting a fine amount that, rather than being collected, must be spent by the utility within a specified time window to rectify the situation that initially led to the violation. This approach would allow the affected utility to make upgrades to critical infrastructure more quickly than if the utility were required to pay a fine to NERC—money they may not see again otherwise. If the end goal is a more reliable and secure bulk power system, this method may allow utilities the freedom needed to upgrade their technology in the most efficient way possible.

Alternatively, FERC and NERC could require the money collected via fines be placed in a trust to be used for improving the resiliency of the electric grid. Once the fund is established, NERC could award a certain sum from the fund in annual, semi-annual, or quarterly increments as a subsidy for utilities to efficiently complete projects. This approach could provide a "happy medium" that would allow for effective enforcement and collection of fines while also facilitating the development of a more robust and secure bulk power system in the long run.

VII. Conclusion

Of all the innovations developed by mankind in the past 200 years, none may be as revolutionary as electricity. In America, essentially every citizen uses

electricity every day, and almost all Americans are serviced by the bulk power system. The BPS is one of the most significant American innovations of the past 100 years. Its storied past provides a model of a robust public/private partnership that has so far withstood the test of time, significant weather events, and rapid industrial change.

While the grid is a positive model of American innovation and public/private partnership, its future is threatened by the rise of the Internet and the ensuing increase in cyberattacks. As joint regulators, FERC and NERC are working diligently to minimize the risk of a cyberattack that could render the grid inoperable. CIP-008 is an important part of that framework, but the latest revision has drastically expanded the scope of cybersecurity compliance requirements and could have a number of unintended consequences. This Note has explored the most critical deficiencies of CIP-008-6, including the absence of any unified definition of what constitutes a reportable "attempted" cybersecurity attack, the potential to drive utilities to focus on compliance activities over security activities, and the burdensome fines that utilities are required to pay if they do not comply with the regulations.

While these deficiencies exist within CIP-008-6, a number of revisions would likely make the standard more effective and enforceable. First, mandating utility participation in CRISP would likely benefit regulators by providing access to data more quickly for analyzing threats, enabling a more proactive response. Participation in CRISP would also benefit the utilities by helping them prudently utilize capital for technology expenses and encouraging the government to develop a center of excellence in detecting and analyzing cybersecurity threats. This Note also explored changing the penalty structure of the CIP standards to provide for a more resilient grid, either by mandating the use of the fine to improve an individual utility's security posture or by holding the funds in trust to encourage utilities to enhance their cybersecurity infrastructure.

The cybersecurity of the grid will continue to be an issue as society advances. As technology evolves and cybersecurity becomes more defined, malicious actors—both foreign and domestic—will be looking for ways to destabilize this critical piece of American infrastructure. FERC and NERC's continued efforts to develop and enforce Critical Infrastructure Protection standards, including CIP-008-6, are a significant piece of the puzzle. Modifying the standard to improve its efficiency will ensure the bulk power system remains reliable and secure for decades to come.