COMMENTS

Cybersecur[ing] the Electric Grid: A Comparative Analysis of Policy Generation, Transmission, and Distribution in the U.S. and EU

Harry Phillips*

* © 2023 Harry Phillips. Junior Member, Volume 25, *Tulane Journal of Technology and Intellectual Property*, J.D. Candidate 2023, Tulane University Law School; B.A. 2016, English, University of Mississippi. The author wishes to thank his wife, Susan, for her continued support, and his fellow *Tulane Journal of Technology and Intellectual Property* members for their help in preparation of this Comment.

I. INTRODUCTION

Don DeLillo is an American novelist known for "explor[ing] the themes of home-spun paranoia and the fantasies that people construct in order to deal with their own sense of powerlessness."[1] Though DeLillo artfully accomplished this in a thematically wide-ranging capacity, he was particularly lauded for his work that addressed the pervasive nature of technology as a motif almost forty years ago.[2] In explaining the motif's significance, DeLillo noted, "[a]s technology advances in complexity and scope, fear becomes more primitive."[3] This is a powerful paradox standing alone. When viewed through the lens of a society subject to a cyberattack on a central power grid, however, envisioning a collective shift from a civil reaction to a primitive one is especially intimidating.

DeLillo's paradox is one that Americans have seen play out in real-time, particularly in the context of natural disasters. In August 2021, Hurricane Ida made landfall in Louisiana. The category four hurricane "slammed the electric grid . . . with its 150 mph (240 kph) winds, toppling a major transmission tower and knocking out thousands of miles of lines and hundreds of substations."[4] In a matter of hours, water treatment plants were "overwhelmed by floodwaters or crippled by power outages," leaving nearly half-a-million residents without water and subjecting an additional quarter of a million residents to boil-water advisories.[5] Coinciding with a heatwave, the deadly "combination of high temperatures and humidity . . . [made the city] feel like 105 degrees

1. Erin Overbey, *Letter from the Archive: Don DeLillo*, THE NEW YORKER (Jan. 3, 2014) http://www.newyorker.com/books/double-take/letter-from-the-archive-don-delillo.

2. 1985 Winners, *National Book Foundation: Presenter of the National Book Awards*, http://www.nationalbook.org/awards-prizes/national-book-awards-1985/ (last visited Mar. 4, 2022) [https://perma.cc/US2S-YDN6] (announcing DeLillo's "White Noise" as a National Book Award winner).

3. Sam Jordison, *White Noise is an Outsider's Look Inside Small-Town Americana*, THE GUARDIAN (May 17, 2016, 9:09 AM EDT), http://www.theguardian.com/books/2016/may/17/white-noise-is-an-outsider-small-town-life-don-delillo [https://perma.cc/7FUV-EDH7].

4. Jay Reeves & Rebecca Santana, *No Power, No Water, No Gasoline: Louisiana Confronts Ida's Aftermath*, NBC NEW YORK (Aug. 31, 2021, 10:52 PM CT), http://www.nbcnewyork.com/news/national-international/thousands-face-weeks-without-power-in-idas-aftermath/3248431/ [https://perma.cc/87BN-AK3J].

5. *Id.*

Fahrenheit."[6] The response? An immediate mobilization of over five thousand National Guard troops and twenty-five thousand utility workers, the erection of mass food and water distribution sites, and curfews enacted "to prevent crime after [the hurricane] devastated the power system and left the city in darkness."[7]

It is indisputable that Hurricane Ida disastrously affected Louisianans. However, it is significant to note that residents were on notice of the impending storm at least three days before it made landfall, allowing them to prepare for the eventual grid collapse.[8] It is likewise indisputable that malicious actors are capitalizing on advances in technology to remotely carry out attacks from behind a computer screen.[9] Because of this, national preparedness for cyberattacks on the power grid and other critical infrastructure has been placed at the forefront of political agendas across the world.[10]

Despite global consensus on the importance of increasing cybersecurity, governments vary in their legislative and regulatory approaches to facilitating the requisite preparedness.[11] This is particularly evident when comparing the American and the European Union (EU) approaches to securing their respective power grids.

This Comment proceeds to compare the two frameworks and ultimately argue that the U.S. regulatory system is better suited to defend

6. *Id.*

7. David Vergun, *National Guard Deployed to Areas Ravaged by Hurricane Ida*, DOD NEWS (Aug. 31, 2021), http://www.defense.gov/News/News-Stories/Article/Article/2757525/national-guard-deployed-to-areas-ravaged-by-hurricane-ida/ [https://perma.cc/Z67D-CC4C]; *see* Reeves & Santana, *supra* note 4.

8. Press Release, Gov. Edwards Declares State of Emergency due to Tropical Storm Ida (Aug. 26, 2021), https://gov.louisiana.gov/index.cfm/newsroom/detail/3367#:~:text=Gov.%20John%20Bel%20Edwards%20has,near%20major%20hurricane%20intensity%20Sunday [https://perma.cc/54QP-3XYY].

9. *See* Michael Riley, *What Happens When Russian Hackers Come for the Electrical Grid*, BLOOMBERG (Jan. 26, 2022, 3:00 AM CT), http://www.bloomberg.com/news/features/2022-01-26/what-happens-when-russian-hackers-cyberattack-the-u-s-electric-power-grid [https://perma.cc/WRV6-7296].

10. Press Release, Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure, White House Briefing Room (July 28, 2021) [hereinafter Biden Press Release], https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ [https://perma.cc/Q7ZA-3EDU]; *see also Critical Infrastructure and Cybersecurity*, EUROPEAN COMMISSION, http://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en (last visited Mar. 5, 2022) [https://perma.cc/JFE9-P3A2] [hereinafter *EU Critical Infrastructure*] (discussing efforts to improve "Network code on cybersecurity" reaching into 2022).

11. Biden Press Release, *supra* note 10; EU Critical Infrastructure, *supra* note 10.

the grid against bad actors. First, it explores the legislative histories and the current state of the respective laws. Second, it evaluates the respective models' effectiveness for ensuring cybersecurity today. Finally, it explains that the advantage of the United States' (U.S.) current regulatory model—as compared to the EU's recently adopted network code—is that U.S.'s model is fully operational and has the capacity to effectively and timely regulate actors with access to bulk electric systems.

II. THE UNITED STATES MODEL

In April 2021, the Biden Administration announced a "100-Day Plan" designed to serve as a "coordinated effort between [Department of Energy (DOE)], the electricity industry, and the Cybersecurity and Infrastructure Security Agency (CISA)."[12] This effort's primary purpose was "confront[ing] cyber threats from adversaries who seek to compromise critical systems that are essential to U.S. national and economic security."[13] Less than thirty days into the 100-Day Plan, owners of the Nation's largest oil pipeline were forced to cease pipeline operations in response to a ransomware attack carried out by a private foreign criminal organization.[14] In the aftermath of the Colonial Pipeline cyberattack, cybersecurity catapulted to the top of national security agendas.[15]

In the months following, President Biden addressed concerns by issuing a National Security Memorandum, meeting with business executives in the private sector, and calling for political leaders across the world to hold cybercriminals accountable for their actions.[16] The National Security Memorandum—"Improving Cybersecurity for Critical Control

12. *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats*, DEP'T OF ENERGY (Apr. 20, 2021), http://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0 [https://perma.cc/NCJ7-T37X].

13. *Id.*

14. Stephanie Kelly & Jessica Resnick-ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, REUTERS (June 8, 2021, 7:06 PM CDT), http://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [https://perma.cc/ZF7S-LMFJ].

15. *See Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 17, 2021).

16. Press Release, Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (Aug. 25, 2021), http://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ [https://perma.cc/QM6W-HVQZ].

Systems"—emphasized the "pilot effort with the Electricity Subsector."[17] The pilot effort aimed to bolster "threat visibility, indications, detection, and warnings, and . . . facilitate response capabilities for cybersecurity in essential control system and operational technology networks."[18] Among the many pivotal organizations charged with this effort, perhaps the two most important organizations, with respect to securing the electricity grid, are the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC).[19]

This section proceeds to analyze the U.S. regulatory framework for ensuring electric grid cybersecurity by (1) establishing the source of FERC's statutory authority while explaining why NERC is a critical party to the regulatory process, and (2) discussing and assessing the current state of the NERC Critical Infrastructure Protection (CIP) Reliability Standards—the driving force behind electric grid cybersecurity.

A. FERC Statutory Authority and the Legislative History of the FERC/NERC Relationship

FERC statutory authority is rooted in the Federal Power Act (FPA).[20] Originally enacted in 1920, the FPA established the Federal Power Commission (FPC).[21] In 1977, the Department of Energy Organization Act established FERC and subsequently transferred functions of the FPC to FERC.[22] These functions included "the establishment, review, and enforcement of rates and charges for the transmission or sale of electric energy . . . under part II of the [FPA], and the interconnection . . . of facilities for the generation, transmission, and sale of electric energy."[23]

Because Part II of the FPA falls under FERC's purview, FERC has jurisdiction over every facility that engages in transmitting electricity in

17. Press Release, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021), http://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cyber security-for-critical-infrastructure-control-systems/ [https://perma.cc/HM23-SH6D].

18. *Id.*; *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats*, *supra* note 12.

19. *About NERC*, NERC, https://www.nerc.com/AboutNERC/Pages/default.aspx (last visited Mar. 11, 2022) [https://perma.cc/KN9P-JER9].

20. 16 U.S.C. § 792.

21. *Id.*

22. 42 U.S.C. § 7134; 42 U.S.C. § 7172.

23. § 7172(a)(1)(B).

interstate commerce.[24] Critical to FERC's regulatory authority over the electric grid cybersecurity is 16 U.S.C. § 824o, which covers "Electric reliability," and provides the following definitions:

> (1) The term "bulk-power system" means— (A) facilities and control systems necessary for operating an interconnected electric energy transmission network . . . .
>
> (2) The terms "Electric Reliability Organization" and "ERO" mean the organization certified by the Commission . . . the purpose of which is to establish and enforce reliability standards for the bulk-power system, subject to Commission review.
>
> (3) The term "reliability standard" means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes . . . cybersecurity protection . . . .
>
> (4) The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.

16 U.S.C. § 824o(a).[25] These definitions, and particularly the provision regarding the Electric Reliability Organization (ERO), provided FERC with the foundation to formally build out the modern regulatory framework for electric grid cybersecurity via their relationship with NERC.

Section 824o also establishes the process for which the ERO becomes certified, FERC's specific jurisdiction over the certified ERO, the criteria for authorizing ERO reliability standards, and the ERO's enforcement powers.[26] In accordance with the certification requirements listed in Section 824o(c), FERC published the requisite qualification criteria and selected NERC as the single ERO in 2006.[27] Within a month of receiving its certification as the sole ERO, NERC formally submitted

24. 16 U.S.C. § 824o(b)(1) (noting also, however, that FERC's jurisdiction does not apply to local distribution facilities or "facilities for the transmission of electric energy consumed wholly by the transmitter").

25. *See infra*, note 33 (defining the updated NERC "Bulk Electric System," which took the place of the FPA's Bulk Power System).

26. § 824o(b)-(e).

27. *See Rules Concerning Certification of the Electric Reliability Organization (Order No. 672)*, 71 Fed. Reg. 8662 (Feb. 17, 2006).

eight Critical Infrastructure Protection (CIP) Reliability Standards for FERC approval.[28] FERC subsequently approved the initial CIP Reliability Standards and "direct[ed] NERC to develop modifications to the CIP Reliability Standards to address specific concerns."[29] Ongoing modifications to the CIP Reliability Standards are the basis for the system that exists today and will continue to shape the system as new threats arise in the future.

B. Current and Future NERC CIP Reliability Standards Framework

There are currently thirteen enforceable CIP Reliability Standards.[30] In addition to the thirteen enforceable Standards, two pending Standards will be enforceable before 2025.[31] The Standards can be thought of as categorical areas of enforcement. As a starting point, CIP-002-5.1a outlines the "BES Cyber System Categorization."[32]

This section discusses the NERC CIP Reliability Standards framework and proceeds in the following order: first, it defines NERC's "Bulk Electric System," including its three-step qualification test, and outlines the BES Cyber System categories; second, this section discusses what this Comment posits are the two most important enforceable standards for directly defending the power grid against cyber threats; and third, it discusses NERC enforcement tools for noncompliance.

1. Definition of the Bulk Electric System, Its Three-Step Test and a Broad Outline of BES Cyber System Categories

The Bulk Electric System is defined as "all Transmission Elements operated at 100 kV or higher and the Real Power and Reactive Power resources connected at 100 kV or Higher," and importantly, "[it] does not include facilities used in the local distribution of electric energy."[33] This

28. *Mandatory Reliability Standards for Critical Infrastructure Protection (Order No. 706)*, 73 Fed. Reg. 7367, 7369 (2008).

29. *Id.*

30. *US Reliability Standards*, NERC, https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx (choose "United States Mandatory Standards Subject to Enforcement") (last visited Mar. 11, 2022) [https://perma.cc/QK66-88XA].

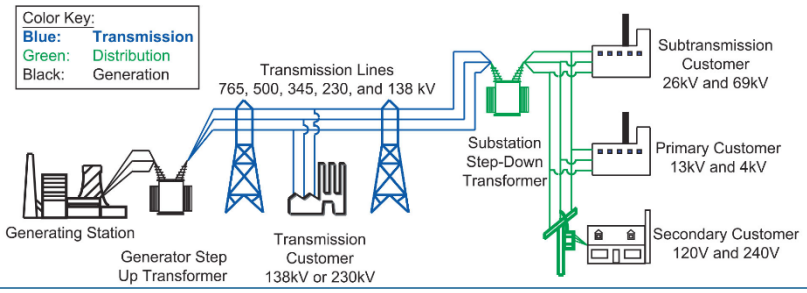
31. *Id.* (choose "United States Standards Subject to Future Enforcement"); *see also Internal Network Security Monitoring for High and Medium Impact Bulk Electric Cyber Systems*, 87 Fed. Reg. 4173 (proposed Jan. 27, 2022).

32. US Reliability Standards, *supra* note 30.

33. *Bulk Electric Systems Definition Reference Document*, *NERC* (Aug. 2018) [hereinafter *BES. Definition Reference*], https://nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf [https://perma.cc/7XRA-8UNP].

definition establishes "bright-line criteria" for the initial determination of whether the component is a BES or non-BES element.[34] Thus, understanding this definition is an important prerequisite to determining whether CIP Reliability Standards apply to the associated BES Cyber Systems.[35]

Figure 1: Power Grid Voltage Schematic Overview[36]



Concerning the CIP Reliability Standards, if the component is a BES Element and satisfies the remaining two steps of the process, then the cyber systems within are subject to NERC jurisdiction. As displayed in Figure 1, facilities subject to NERC jurisdiction are generally those associated with power generation and transmission before the power is "stepped-down" for local distribution.

To identify a BES Element, the first step requires determining whether a BES Element meets the requisite 100 kV threshold, which serves as the "overall demarcation point between BES and non-BES Elements."[37] The second step "involves applying the specific inclusions and provides additional clarification for identifying specific elements that are included in the BES."[38] The final step identifies what BES Elements or "groups of elements" should be excluded from the BES based on a specific set of situations.[39]

34. *Id.* at v (internal quotation marks omitted).

35. *Id.* (noting "[t]he application of the bright-line BES definition is a three-step process that . . . will identify the vast majority of BES Elements in a consistent manner [and] be applied on a continent-wide basis," and defining "BES Element," as "Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section or transmission line").

36. *Understanding the Grid*, NERC (Aug. 2013), http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf [https://perma.cc/HHY2-9YTC].

37. *BES Definition Reference*, *supra* note 33, at v.

38. *Id.* (noting that there are five inclusions to consider).

39. *Id.*

After making the initial determination that there is a BES Element and, thus, that CIP Reliability Standards apply to the cyber systems within, it is necessary to categorize the systems associated with the BES Element under the BES Cyber System Categorization model found in CIP-002-5.1a.[40] The purpose of this model is to "support appropriate protection against compromises that could lead to misoperation or instability in the BES."[41] The model sets forth three "rating" categories—high impact, medium impact, and low impact—and provides specific criteria for facility owners to consider when making assessments.[42] Notably, "discrete identification of BES Cyber Systems [is only required] for those in the high impact and medium impact categories."[43] In addition, the standard provides that facility operators should restrict the scope of their assessments to "BES Cyber Systems that would impact the reliable operation of the BES," and those that, "if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise."[44] Although these restrictions prevent an overly burdensome system, there is cause for concern on the basis that it creates a gap in cybersecurity protection for critical infrastructure.[45]

C. The Most Critical Currently Enforceable CIP Reliability Standards: CIP-007-6 and CIP-005-7

Each CIP Reliability Standard in force plays an important role in directly or indirectly contributing to power grid cybersecurity. However, this Comment argues that the two most important CIP Reliability Standards to defend the grid against a cyberattack are "CIP-007-6 (Systems Security Management)" (CIP-007) and "CIP-005-6 (Cyber

40. CIP-002-5.1a, Cyber Security-BES Cyber System Categorization, NERC (2016), https://nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf [https://perma.cc/P8Y6-G8PW][hereinafter CIP-002].

41. *Id.* at 1.

42. *Id.* at 14-16, 23 (defining "High Impact Rating" as "BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform [certain functional obligations]"; and providing requisite standards for determining "Medium Impact Rating" and "Low Impact Rating"); *see also infra*, notes 49, 50 (defining "BES Cyber System" and "Control Center").

43. *CIP-002*, *supra* note 40, at 5.

44. *Id.* (describing these additional categories as "Reliable Operation of the BES" and "Real-time Operations").

45. *See infra*, notes 68-59.

Security—Electronic Security Perimeter(s))" (CIP-005) because these measures play a more active role in grid cybersecurity.[46]

FERC approval for CIP-007 was granted in 2016 via FERC Order No. 822.[47] The purpose of CIP-007 is "[t]o manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise."[48] The standard applies to high impact and medium impact BES Cyber Systems.[49] Additionally, CIP-007 applies to medium impact BES Cyber Systems located at control centers and "medium impact BES Cyber Systems with External Routable Connectivity."[50] Lastly, CIP-007's scope extends to "Electronic Access Control or Monitoring Systems" (EACMS), "Physical Access Control Systems" (PACS), and "Protected Cyber Assets" (PCA).[51]

CIP-007 includes a list of applicable systems, "documented process(es) that collectively include each of the applicable requirement parts," and specific measures responsible entities should take to adhere to

46. *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 81 Fed. Reg. 4177, 4177 (2016) [hereinafter Order No. 822]; *Supply Chain Risk Management Reliability Standards*, Order No. 850, 82 Fed. Reg. 53992, 53992 (2018) [hereinafter Order No. 850].

47. 81 Fed. Reg. 4177.

48. CIP-007-6, Cyber Security–Systems Security Management NERC (2016) [hereinafter CIP-007], https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf [https://perma.cc/2J5J-QJRL].

49. *Id.*; *see Glossary of Terms Used in NERC Reliability Standards*, *NERC* (Feb. 8, 2005) [hereinafter *NERC Glossary*] (last updated Sept. 21, 2022), http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf [https://perma.cc/QTP5-XRTS] (defining "BES Cyber System" as "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity"; and defining "BES Cyber Asset" as "A Cyber Asset that if rendered unavailable . . . would, within 15 minutes of its required operation . . . adversely impact one or more Facilities . . . Each BES Cyber Asset is included in one or more BES Cyber Systems").

50. *CIP-007*, *supra* note 48, at 4-5; *see also NERC Glossary*, *supra* note 42 (defining "Control Center" as "One or more facilities hosting operating personnel that monitor and control the Bulk Electronic System (BES) in real-time to perform the reliability tasks of: 1) a Reliability Coordinator . . . ."; and defining "External Routable Connectivity" as "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter").

51. *CIP-007*, *supra* note 48, at 4-5; *see NERC Glossary*, *supra* note 42 (defining "EACMS" as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems"; defining "PACS" as "Cyber Assets that control . . . access to the Physical Security Perimeter[s], exclusive of locally mounted hardware or devices . . . such as motion sensors, electronic lock control mechanisms, and badge readers"; defining "PCA" as "One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter").

the listed requirements.[52] Among the standard's systems security management requirement categories are Ports and Services, Security Patch Management, Malicious Code Prevention, Security Event Monitoring, and System Access Control.[53] Monitoring each of these categories is critical for cyberattack prevention because a compliance lapse in any individual category within this standard could provide a bad actor with easy access to common attack vectors used in carrying out a cyberattack.[54]

Notably, the application of the Systems Security Management protocols does not currently extend to low impact BES Cyber Systems. During the Notice of Proposed Rulemaking comment period, NERC and various other participants maintained that this should remain the status quo because of the low risk that a compromised low impact BES Cyber System presents to the BES as a whole.[55] FERC disagreed on the basis that, "even if a [firewall or other security devices] installed at a Low Impact Electronic Access Point successfully logged suspicious network traffic, there is no assurance that a responsible entity would have processes in place to take swift action to prevent malicious code from spreading."[56] Further, FERC noted that NERC was charged with incorporating system security management controls for monitoring low impact BES Cyber Systems.[57]

Extending compliance protocols to low impact BES Cyber Systems is heavily contested on the basis that it will "impose a reporting burden on a much larger group of entities."[58] However, this extension is critical to secure the power grid against future cyberattacks. Future expansion of CIP Reliability Standards, and particularly CIP-007, should include low impact BES Cyber Systems to mend current "gap[s] in the protections under the CIP Reliability Standards."[59] The FERC/NERC-grapple over

52. *CIP-007*, *supra* note 48, at 6.

53. *See generally id*. (defining the various applicable systems, requirements, and measures for each category).

54. *See generally What Is an Attack Vector*, FORTINET, http://www.fortinet.com/resources/cyberglossary/attack-vector (last visited Apr. 2, 2022) [https://perma.cc/6UM2-74K3] (listing common types of attack vectors as including compromised credentials, malware, and unpatched applications or servers).

55. *See* 81 Fed. Reg. 4177, at 4179.

56. *Id*. at 4182.

57. *Id*. at 4180; *see NERC Glossary*, *supra* note 49 (defining "Electronic Access Point" as "A Cyber Asset Interface on an Electronic Security Perimeter [(ESP)] that allows routable communication between Cyber Assets outside an [ESP] and Cyber Assets inside an [ESP]").

58. *See* 81 Fed. Reg. 4177, at 4188 (discussing the financial costs of extensive compliance protocols being extended to Low Impact BES Cyber Systems).

59. *Id*. at 4179.

the necessity to address gaps in protection extended to Order No. 850 in 2018, which promulgated CIP-005—"Cyber Security—Electronic Security Perimeter(s)."[60]

The purpose of CIP-005 is, "[t]o manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."[61] The NERC Glossary of Terms defines "Electronic Security Perimeter" (ESP) as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."[62] CIP-005 applies to each of the "Applicable Systems" covered by CIP-007, but also applies to high and medium impact BES Cyber Systems with Dial-up Connectivity as well as high impact BES Cyber Systems with External Routable Connectivity.[63] Notably, the dispute over whether to apply CIP Reliability Standards to low impact BES Cyber Systems was not addressed in the 2022 CIP-005 modifications.[64]

Requirement categories encompassed by CIP-005 include the Electronic Security Perimeter, Remote Access Management, and Vendor Remote Access Management for EACMS and PACS.[65] Among the remote access management requirements are multi-factor authentication, procedures "for determining active vendor remote access sessions," and

60. *See* 82 Fed. Reg. 53992, at 53992; *see also FERC Order Approving CIP-005-7, Docket No*. *RD21-2-000*, 174 FERC ¶ 61,193 (Mar. 18, 2021), http://cms.ferc.gov/sites/default/files/2021-03/E-17-RD21-2-000.pdf [https://perma.cc/FA3B-NJKA] (approving modifications to CIP-005-6).

61. *CIP-005-7*, *Cyber Security–Electronic Security Perimeter(s)*, *NERC* (effective Oct. 1, 2022) [hereinafter *CIP-005*], https://www.nerc.com/_layouts/15/PrintStandard.aspx [https://perma.cc/A332-VQEX].

62. *NERC Glossary*, *supra* note 49 (defining "Electronic Security Perimeter"); *see also What is Routing? | IP Routing*, CLOUDFLARE http://www.cloudflare.com/learning/network-layer/what-is-routing/ (last visited Apr. 4, 2022) [https://perma.cc/K3AQ-ZTYG] (defining protocol and routing protocol as follows: "a protocol is a standardized way of formatting data so that any connected computer can understand the data. A routing protocol is a protocol used for identifying or announcing network paths").

63. *CIP-005*, *supra* note 61, at 4; *see CIP-007*, *supra* note 48 (listing CIP-007's applicable systems); *see NERC Glossary*, *supra* note 49 (defining "Dial-up Connectivity" as "A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link").

64. 174 FERC ¶ 61,193 at 61,193.

65. *CIP-005*, *supra* note 61, at 6-13; *see NERC Glossary*, *supra* note 42 (defining "Interactive Remote Access" as "originat[ing] from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's [ESPs] or at a defined Entry Access Point (EAP)"); *see also NERC Glossary*, *supra* note 42 (defining "EACMS" and "PACS").

procedures for terminating "active vendor remote access."[66] Compliance with these categories is critical to ensuring cybersecurity because they govern "Cyber Assets used or owned by vendors, contractors, or consultants."[67] This access is particularly important due to the "threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, [and] the threat that a compromise at a trusted vendor could traverse over unmonitored connection into a responsible entity's BES Cyber System."[68] The merits of this concern are noteworthy because they are broadly analogous to the method used by the hackers in May 2021 Colonial Pipeline cyberattack.[69]

D. NERC Enforcement Tools for Noncompliance

Compliance protocols under CIP-005 mirror those of CIP-007. Both standards include a "Compliance Monitoring Process" that requires responsible entities to "keep data or evidence to show compliance" and prescribes a "Compliance Monitoring and Assessment Process[]" for the entities to reference.[70] Where a responsible entity fails to comply with a CIP Reliability Standard via the prescribed protocols, NERC "shall determine and may levy monetary and non-monetary penalties."[71] The maximum monetary penalty NERC can assess is "equal to [the] current inflation-adjusted maximum civil monetary penalty set forth in 18 CFR § 385.1602(d)."[72] Notably, this amount is currently set at $1,388,496 per day; however, the NERC Sanction Guidelines stipulate that there must be a "reasonable relation to the seriousness of the violation(s) and mitigate overly burdensome penalties."[73]

66. *Id.* at 10-11.

67. *NERC Glossary*, *supra* note 49 (defining "Interactive Remote Access").

68. 82 Fed. Reg. 53992, at 53994.

69. *See* Kelly & Resnick-ault, *supra* note 14 (noting that hackers "were able to get into the system by stealing a single password" and that "the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place").

70. *See CIP-007*, *supra* note 48, at 26 (listing the Compliance Monitoring and Assessment Process as follows: Compliance Audits, Self-Certifications, Spot Checking, Compliance Violation Investigations, Self-Reporting, and Complaints).

71. *Sanction Guidelines of the North American Electric Reliability Corporation* 3, *NERC* (effective Jan. 19, 2021) [hereinafter *NERC Sanction Guidelines*], http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%204B%20effective%2020210119.pdf [https://perma.cc/5QC7-GLJB].

72. *Id.* at 4.

73. 18 C.F.R. § 385.1602 (2022); *NERC Sanction Guidelines*, *supra* note 71, at 4.

III. THE EUROPEAN UNION MODEL

Member states of the European Union (EU), EU neighbor countries, and the EU itself are collectively implementing changes to bolster the security of their electric grids in response to various cybersecurity threats.[74] Among significant cyber incidents contributing to the push for a more secure grid was the cyberattack on the Ukrainian power grid in 2015.[75] Notably, the EU electric grid provides power to over 600 million people across forty countries.[76] Because of this, comparing the American and EU policies might seem superficially illogical; however, "most of the interconnected countries [in Europe] follow the same framework and policies in electrical energy generation, transmission and distribution . . . [and] the non-EU countries follow the same rules."[77] Additionally, like NERC's role as the FERC-appointed regulator, the EU Agency for the Cooperation of Energy Regulators (ACER) and the European Network of Transmission System Operators-Electricity (ENTSO-E) serve together in the same capacity as FERC/NERC by "establishing guidelines for trans-European energy Infrastructure."[78]

This section analyzes the current EU regulatory framework for ensuring electric grid cybersecurity by (1) examining the most relevant sources of statutory authority, and (2) discussing the critical role ACER and ENTSO-E play in establishing an electric grid cybersecurity network code.

A. EU Legislative History and Relevant Sources of Statutory Authority for Electric Grid Cybersecurity

The EU has taken multiple legislative measures to boost cybersecurity across the region in the last twenty years. The foundational basis for the ongoing modifications is Council Directive 2008/114/EC

74. *See generally* European Commission Press Release IP/20/2391, New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient (Dec. 16, 2020).

75. Cybersecurity of critical energy infrastructure, EUR. PARL. DOC. PE 642.274 (2019) (noting "hackers penetrated the computer system of a western Ukrainian power utility, and cut off the electricity to some 225 000 people").

76. Nisheeth Singh, *The European Interconnected Network: A Case Study of Institutional Requirements for a Successful International Grid Interconnection 5*, NAPSNET SPECIAL REPORTS, (2020), http://nautilus.org/wp-content/uploads/2020/10/Singh-European-Grid-Interconnections-SR-Oct-5-2020.pdf [https://perma.cc/C493-XHZG].

77. *Id.* at 7.

78. *Id.* at 10.

(2008 Directive).[79] The 2008 Directive, which covers the "identification and designation of European critical infrastructures and the assessment of the need to improve their protection," applies to the energy and transport sectors and specifies the electricity subsector as including, "[i]nfrastructures and facilities for generation and transmission of electricity in respect of supply electricity."[80] In addition, the 2008 Directive assigns "primary and ultimate responsibility" for "European Critical Infrastructures" (ECIs) to ECI owners and operators.[81] In the years since the 2008 Directive, there has been continued reform to ECI cybersecurity with respect to the power grid has come through the following legislative acts: Recommendation (EU) 2019/553, Regulation (EU) 2019/881, Regulation (EU) 2019/941, and Regulation (EU) 2019/943.[82]

B. Recommendation (EU) 2019/553

Commission Recommendation (EU) 2019/553 (Recommendation), which covers "cybersecurity in the energy sector," noted that "part of [the] energy transition . . . technological progress . . . [is] turning Europe's power grid into a 'smart grid'" which as a result, "exposes the energy system to cyberattacks and incidents which may jeopardize the security of energy supply."[83] To address this, the Recommendation established "guidelines that Member States and key stakeholders . . . should take into account when making decisions about infrastructure," including "cybersecurity risk analysis and preparedness."[84] In doing so, the Recommendation emphasized, "Electricity grids . . . are strongly interconnected across Europe and a cyber-attack creating an outage or disruption in a part of the energy system might trigger far-reaching

79. Council Directive 08/114, 2008 O.J (L345/75) (EC) [hereinafter 2008 Directive]; *see also* Cybersecurity of Critical Energy Infrastructure, *supra* note 75, at 1.

80. *2008 Directive*, *supra* note 79, art. 3(3), Annex I.

81. *Id.* at pmbl. para. (4), (6).

82. *See Types of legislation*, EUROPEAN UNION, http://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (last visited April 4, 2022) [https://perma.cc/4H39-2U52] (defining "Regulation" as "a binding legislative act [that] must be applied in its entirety across the EU"; defining "Directive" as "a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals"; defining "Recommendation" as "not binding . . . . [A] recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed").

83. Council Recommendation 19/553, pmbl. para. (1), 2019 O.J. (L 96/50) [hereinafter Recommendation 19/553].

84. Cybersecurity of Critical Energy Infrastructure, *supra* note 75, at 5.

cascading effects into other parts of that system."[85] After publishing the (non-binding) Recommendation in April 2019, binding Regulations 2019/941 and 2019/943 were enacted.[86]

C. Regulation (EU) 2019/941

Regulation (EU) 2019/941 was published alongside Regulation (EU) 2019/943 in June 2019, just two months after Commission Recommendation 2019/553.[87] The Regulation, which covers "risk-preparedness in the electricity sector," emphasized, "[i]n a context of interlinked electricity markets and systems, electricity crisis prevention . . . cannot be considered to be a purely national task . . . [and] [a] common framework of rules and better coordinated procedures are needed."[88] To establish the requisite rules for risk preparedness the Regulation maintains is necessary, it charged ACER with working alongside the ENTSO-E to "develop and update a common methodology for risk identification."[89] Importantly, Regulation 2019/941 is limited to rules related to the prevention of, preparation for, and management of electricity crises; by contrast, Regulation 2019/943 sets rules for the actual regulation of the EU internal electricity market via mandating the establishment of a network code for cybersecurity.[90]

D. Regulation (EU) 2019/943

Among the purposes of Regulation 2019/943 is to "[f]acilitate the emergence of a well-functioning . . . market, contributing to a high level of security of electricity supply."[91] To aid in facilitating a high level of security of electricity supply, the Regulation charged ENTSO-E to "[p]romote cyber security and data protection in cooperation with relevant authorities and regulated entities."[92] In doing so, the Regulation mandated that ENTSO-E and ACER establish a network code that sets "sector-specific rules for cyber security aspects of cross-border electricity flows,

85. *Recommendation 19/553*, *supra* note 83, at Cascading Effects (6).

86. *See Types of legislation*, *supra* note 82 (distinguishing the legal effect of a regulation from that of a recommendation).

87. *See generally* Council Regulation 19/941, 2019 O.J. L 158/1 (EU) [hereinafter Regulation 19/941]; Council Regulation 19/943, 2019 O.J. L 158/54 (EU) [hereinafter Regulation 19/943].

88. Regulation 19/941, *supra* note 837, at pmbl. para. (3).

89. *Id.* at pbml. para. (13).

90. *Id.* at pbml. para. (6); Cybersecurity of Critical Energy Infrastructure, *supra* note 75.

91. Regulation 19/943, *supra* note 837, art. 1(d).

92. *Id.* art. 30(1)(n).

including rules on common minimum requirements, planning, monitoring, reporting and crisis management."[93] In January 2022, ENTSO-E formally submitted a proposal for this mandated Network Code for ACER review.[94]

1. Ongoing Efforts by ACER and ENTSO-E in Establishing a Cybersecurity Network Code in the EU

Becoming enforceable in 2009, the Third Energy Package is the source of authority for ACER and ENTSO-E detailing their roles in establishing a network code for cybersecurity.[95] Though it has since been revised, the original aim of the Third Energy Package was to "improv[e] the functioning of the internal energy market and resolve certain structural problems."[96] It accomplished this by covering five areas, including the respective responsibilities of ACER and ENTSO-E.[97] This section (1) outlines the responsibilities of ACER and ENTSO-E and (2) discusses the current state of the Network Code on Cybersecurity.

E. Historical Overview and Responsibilities of ACER and ENTSO-E

ACER was established by the EU as "independent from the Commission, national governments, and energy companies," to "help different national regulators cooperate and ensure the smooth functioning of the internal energy market."[98] Notably, ACER's responsibilities

93. *Id.* art. 59(2)(e); *see also* Cybersecurity of Critical Energy Infrastructure, *supra* note 75 (defining "Network Code" as "binding rules for the EU energy system developed by [ACER] in cooperation with the European networks of transmission and distribution operators," and adding "They are approved by the EU Member States in a comitology procedure and adopted by the Commission as implementing regulations").

94. *See ENTSO-E and the EU DSO Entity Submit the Network Code on Cybersecurity for ACER Review*, EU DSO ENTITY (Jan. 14, 2022), https://www.eudsoentity.eu/news/posts/2022/january/entso-e-and-the-eu-dso-entity-submit-the-network-code-on-cybersecurity-for-acer-review/ [https://perma.cc/FP5F-JB2T] (noting that ENTSO-E did so in collaboration with the EU DSO Entity).

95. *Third Energy Package*, EUR. COMM'N, http://energy.ec.europa.eu/topics/markets-and-consumers/market-legislation/third-energy-package_en (last visited Apr. 5, 2022) [https://perma.cc/Y74W-HYUT] (noting, however, that since entering into force, "Electricity market design has replaced the electricity part" and the Electricity Regulation (EC) No 714/2009 and the ACER Regulation (EC) No 713/2009 were revised).

96. *Id.*

97. *Id.* (listing the five areas as "unbundling, independent regulators, ACER, cross-border cooperation and open and fair retail markets," and noting that cross-border cooperation is accomplished via ENTSO-E).

98. *Id.* (noting ACER's responsibilities include "drafting guidelines for the operation of . . . electricity networks"; "reviewing the implementation of EU-wide network development

include monitoring the execution of ENTSO-E's tasks, reviewing ENTSO-E's proposed network codes, and advising the European Commission.[99] Additionally, ACER is considered a "[c]ommunity body with legal personality" that "shall enjoy the most extensive legal capacity accorded to legal persons under the law . . . and be able to acquire or dispose of movable or immovable property and be a party to legal proceedings."[100] With respect to cybersecurity, the agency contributes in three primary capacities: (1) "Advising on EU legislation and rules"; (2) "Sharing information among energy regulators and capacity building" and (3) "Contribut[ing] to EU and international collaboration" via its cybersecurity experts.[101]

ENTSO-E was created through Regulation (EC) No 714/2009 (Regulation 714), which covers "conditions for access to the network for cross-border exchanges in electricity."[102] Regulation 714 established that "all transmission system operators shall cooperate at [the] Community level through [ENTSO-E]."[103] To do this, the Regulation charged ENTSO-E with working alongside ACER to create various network codes for cross-border issues.[104] Once network codes are in force, ENTSO-E oversees their implementation across EU Member States.[105] Notably, ACER is charged with ensuring that ENTSO-E "monitor[s] and analyse[s] the implementation."[106] Finally, concerning "Penalties," Regulation 714 establishes that "Member States shall lay down rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that provisions are implemented."[107]

---

plans"; "deciding on cross-border issues if national regulators cannot agree or if they ask it to intervene"); *see also* Council Regulation 713/09, 2009 O.J. L 211/1 (EC) [hereinafter Regulation 713/2009].

99. Regulation 713/09, *supra* note 99, at pmbl. (7), (9).

100. *Id.* art. 2(1)-(2).

101. *ACER and Cybersecurity*, ACER, http://documents.acer.europa.eu/en/Electricity/CLEAN_ENERGY_PACKAGE/Pages/ACER-and-cybersecurity.aspx (last visited Apr. 5, 2022) [https://perma.cc/TG3N-E4KS].

102. *See generally* Council Regulation, 714/09, 2009 O.J. L 211/15 (EC) [hereinafter Regulation 714/2009].

103. *Id*. art. 4.

104. *Id*. at pmbl. (6) ("[ACER] should have a role in reviewing, based on matters of fact, draft network codes, including their compliance with the framework guidelines, and it should be enabled to recommend them for adoption by the Commission.")

105. *Id*. art. 9(1).

106. *Id*.

107. *Id*. art. 22 (noting the "penalties provided for must be effective, proportionate and dissuasive").

F. The Current State of the Network Code on Cybersecurity

As previously noted, ENTSO-E submitted a draft network code covering the cybersecurity aspects of cross-border electricity flows (network code or NCCS) to ACER in January 2022.[108] In June 2022, ACER formally endorsed a revised draft of the network code and in July 2022 the Board of Regulators "provided a favourable opinion" that was subsequently adopted by the European Commission.[109] Because of this, each country connected to the intra-EU grid must begin to implement cybersecurity protocols and regulations in accordance with guidelines and timelines provided for in the NCCS.

The legislative authority for the revised NCCS was provided by ACER per Regulation 2019/943.[110] Provisions in the NCCS address the requisite scope of the network code, provide a detailed outline of the desired cybersecurity risk assessment for cross-border electricity flows, and detail other frameworks and processes ACER deemed as necessary pieces of the network code.[111] The Framework Guideline was originally sourced from "extensive preparatory work," including "the recommendations of the Smart Grid Task Force Expert Group 2 report and [ENTSO]," and "was subject to public consultation for two months."[112]

The now-approved network code applies to various EU-based public and private entities as well as to "critical service providers" based outside the EU when delivering services into the EU "which may affect cross-border flows directly or indirectly."[113] Imperative to the NCCS's success will be the respective roles of national regulatory authorities (NRAs) and the competent authorities for cybersecurity (CS-NCAs).[114] Importantly,

108. *See ENTSO-E and the EU DSO Entity Submit the Network Code on Cybersecurity for ACER Review, supra* note 94.

109. *ACER*, *Framework Guideline on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows* 2 (July 22, 2021) [hereinafter Framework Guideline], https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20SectorSpecific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf [https://perma.cc/XU26-5BGS].

110. *Id.*

111. *Id.* at 6.

112. *Id.*

113. *Id.* at 10-11.

114. *Network Code for Cybersecurity Aspects of Cross-Border Electricity Flows,* ENTSO-E, 6, 9 (proposed Jan. 14, 2022) [hereinafter Proposed Network Code], http://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20CS/220114_NCCS_Legal_Text.pdf [https://perma.cc/9MA2-LEWV].

these organizations will work in tandem with ACER and other entities "[to monitor] the implementation of the application of the cybersecurity standards" of the proposed network code.[115]

CS-NCAs and NRAs will be responsible for identifying "all high-impact and critical-impact entities" in their respective states.[116] The identification of high-impact and critical-impact entities is vital to the success of the proposed network code because these categories, like those utilized by the American system, will determine what criteria operators must consider in order to comply with the cybersecurity risk framework established in the proposed network code.[117] A notable gap in the revised network code, however, is that high- and critical-impact thresholds remain vaguely defined on the basis that proposed definitions will follow "[w]ithin 9 months after entry into force of the [NCCS]."[118] Likewise, the "Common Electricity Cybersecurity Framework" outlines requisite categorical elements, but detailed requirements are contingent upon future proposals in accordance with a prescribed timeline.[119] As a result of this, the full scope of the revised network code's compliance protocols is currently unclear and makes a comparative analysis of regulatory strong points between the two frameworks moot. From a risk mitigation perspective, the lack of detailed technical requirements in the network code is a significant gap because it will ultimately require an extensive amount of time and debate before finalization and the risk of a cyberattack is imminent.

IV. WHICH MODEL IS MOST EFFECTIVE FOR DEFENDING AGAINST A CYBERATTACK ON THE POWER GRID?

In its current state, the American cybersecurity framework is most effective for defending against a cyberattack on the power grid for the simple reason that efforts to implement a framework designed to protect the intra-EU power grid, though formally adopted by the European Commission, are still ongoing and subject to extensive implementation timelines. Although this answer might seem anti-climactic, it is a noteworthy point for three reasons. First, the United States and the EU have each been implementing legislative changes to bolster electric grid cybersecurity for close to a decade. However, the first proposed CIP

115. *Id*. art. 16(2)(b).
116. *Id*. art. 50(2).
117. *See id*. art. 17; *see also CIP-002*, *supra* note 40.
118. *Network Code*, *supra* note 114, at arts. 4(11), 4(30), 17(1).
119. *See id*. at Title IV.

Reliability Standards were submitted by NERC for FERC approval within a month of being certified as the ERO in 2006 and original CIP Standards have been revised concurrently as FERC and NERC see fit.[120] In the EU, on the other hand, critical infrastructures were identified in 2008 and a cybersecurity strategy was in place as early as 2013, but the regulation charging ACER and ENTSO-E to develop a network code on cybersecurity for cross-border flows of electricity was enacted in 2019 and, although there is now an approved system in place for regulating cybersecurity for cross-border electricity flow, it is subject to various implementation timelines and required studies or reports.[121]

Second, the legitimate threat of a cyberattack on critical infrastructure is not such a novel concept or unlikely reality that it justifies the EU's comparatively longer legislative enaction and implementation processes. For example, as early as 2008 the Central Intelligence Agency "knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply to four foreign cities."[122] Likewise, as early as 2013 the Department of Homeland Security reported that "the U.S. electrical grid [was] constantly being probed by multiple actors, including Iran."[123] While recent reports indicate that bad actors are carrying out more complex cyberattacks, the threat of attacks has been a constant reality for the better part of twenty years.[124]

Third, the EU's delay in implementing the network code is noteworthy because enacting highly technical and effective legislation in a short period is not an unprecedented accomplishment. The EU accomplished exactly this in 2016 via the enaction of its General Data Protection Regulation (GDPR).[125] The GDPR, which requires extensive regulatory oversight by each EU Member State, was formally adopted by the European Parliament in 2014, enacted in 2016, and transposed into

120. 71 Fed. Reg. 8662 (noting FERC published requisite qualification criteria and selected NERC as the single ERO in 2006); Cybersecurity of Critical Energy Infrastructure, *supra* note 75, at 5 (discussing the EU's 2013 cybersecurity strategy); *see also* 73 Fed. Reg. 7367.

121. *See* 71 Fed. Reg. 8662.

122. *Significant Cyber Incidents Since 2006*, CSIS, http://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf (last visited Apr. 5, 2022) [https://perma.cc/L5LR-X98C].

123. *Id.*

124. *See generally id.*

125. *See generally* Council Regulation 16/679, 2016 O.J. L 119/1 (EU) [hereinafter Regulation 16/679].

the law of each EU Member State by 2018.[126] The EU's ability to enact this regulation, which it regards "as a gold standard all over the world," shows that the EU is capable of more efficiently enacting substantive legislation than what has been displayed for the case of the network code on cybersecurity aimed at cross-border data flows.[127]

Although this Comment has criticized the proposed (and subsequently revised) network code's lack of in-depth technical requirements and slow implementation timeline, the author acknowledges that it is not without positive features. Particularly positive elements of the network code include regional cybersecurity response exercises, collaborative efforts among regulatory authorities at all levels, recovery of costs offsetting the implementation of the new system, and considerations for data protection.[128]

As the NCCS is implemented, regulatory requirements for regional cybersecurity exercises will actively prepare transmission and distribution operators to identify and react to cyber threats. Additionally, provisions offsetting implementation costs will increase the expediency with which TSOs and DSOs implement the network code because it eases the associated financial burden.[129]

The most impactful shared benefit between the NERC CIP Reliability Standards and the NCCS, however, is the respective delegation of penalty enforcement power to the regulatory authorities. The revised network code delegates this power to regulatory authorities in accordance with Directive (EU) 2019/944.[130] Directive (EU) 2019/944, which covers "common rules for the internal market for electricity," provides that regulatory authorities have the power "to impose effective proportionate and dissuasive penalties on electricity undertakings not complying with their obligations under . . . Regulation (EU) 2019/943 . . . including the power to impose . . . penalties of up to 10% of annual turnover."[131] Because monetary penalties assigned to NERC are limited to $1,388,496.00 per day under 18 CFR § 385.1602(d), regulatory agencies in the EU might have the upper hand in the context of

126. *The History of the General Data Protection Regulation*, EDPS, http://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Apr. 6, 2022) [https://perma.cc/DR49-B4AU].

127. *Id.*

128. *Proposed Network Code*, *supra* note 114, arts. 46-48, 16, 10, 49.

129. *Id.* art. 10(1) ("Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms.").

130. *See id.* art. 2(1)(i) (noting that "Regulatory Authorities" exist pursuant to Article 59 of Directive (EU) 2019/944).

131. Council Directive 19/944, art. 59(3)(d), 2019 O.J. L 158/125 (EU).

enforcement tools when the network code is fully implemented.[132] Ultimately, however, the American model remains more effective in defending against a cyberattack due to its fully operational and implemented status.

V. CONCLUSION

This Comment compared the American and EU frameworks for electric grid cybersecurity by exploring legislative histories and the current states of the respective laws and regulatory schemes. Ultimately, this Comment explains that the regulatory model in the United States is better prepared to defend against a cyberattack on its power grid because the NERC CIP Reliability Standards are fully in effect and the regulatory scheme of entities with access to the bulk electric system provides a more effective and timely response than the EU's regulatory scheme. Though designing and implementing a regulatory scheme as a single country is admittedly less arduous than as a union of countries, the imminent threat of cyberattacks on critical infrastructure has become well-established and increasingly devastating in the last twenty years. Because of this, there is no merit in quibbling over the excuse that the EU must navigate more bureaucratic and legislative hoops to implement a cybersecurity framework for defending the intra-EU power grid—it simply must get done.

Some may object to expediting the network code because such measures will serve as a short-term fix to a long-term problem. However, these objectors should consider that preventative steps proactively implemented in the immediate future will better mitigate the fallout of the EU reacting to a cyberattack without the aid of published guidance. As General Patton once said, "A good plan violently executed now is better than a perfect plan next week."[133]

132. *See NERC Sanction Guidelines*, *supra* note 71.

133. Gary A. Klein, *Strategies of Decision Making*, 65(5) MIL. REV. 56, 56 (1989).