IMPROVING NATIONAL SECURITY ONE REPORT AT A TIME: FERC ORDER NO. 848

I. INTRODUCTION

In recent years, there have been an increasing number of attacks by foreign cyber hackers on critical infrastructure in the United States.[1] Particularly since the COVID-19 pandemic, cyber threats have been on the rise globally across a variety

1. Brian Naylor, *Russia Hacked U.S. Power Grid – So What Will The Trump Administration Do About It?*, NAT'L PUB. RADIO: POLITICS (Mar. 2018), https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it.

of critical infrastructure sectors.[2] For example, some of the reported incidents show that a hacker attempted to poison the water supply of a small city in Florida,[3] cyber weapons leaked from U.S. sources (federal agencies, the private sector, and critical infrastructure),[4] and North Korea attempted to hack Pfizer for information regarding the COVID-19 vaccine.[5] Growing awareness for these types of issues has spurred movements to mitigate potential harms in a variety of ways, such as changing how voting machines work so that they no longer permit wireless connectivity.[6] With this increase in cyberactivity, the United States is paying even greater attention to the cybersecurity of our electricity grid, as nearly all industries depend on the energy sector.[7]

Notable cyberattacks on the energy industry include an event from the summer of 2017 where Russian hackers conducted a "multistage intrusion campaign" to gain access to the control system of a U.S. power plant through "common hacking techniques such as malware and spear-phishing."[8] According to the head of counterintelligence under the Director of National Intelligence during the Obama administration, these hackers were not just trying to observe the system.[9] He continued by stating that the hackers were essentially "placing the tools that they would have to place in order to turn off the power," and he does not believe the United States is prepared to deal with this type of threat.[10] Awareness regarding cybersecurity vulnerabilities, expanding existing securities, and removing existing

---

2. *See, e.g.*, Dan Lohrmann, *2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic*, GOV'T TECH. (Dec. 2020), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html; MonsterCloud, *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, PR NEWSWIRE: CISION (Aug. 2020), https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html; David Grober, *Roundup: COVID-19 Pandemic Delivers Extraordinary Array of Cybersecurity Challenges*, ZDNET: SPECIAL FEATURE (Nov. 2020), https://www.zdnet.com/article/roundup-the-coronavirus-pandemic-delivers-an-array-of-cyber-security-challenges/; Tope Aladenusi, *COVID-19's Impact on Cybersecurity*, DELOITTE: ARTICLES (Mar. 2020), https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html.

3. Frank Bajak, Alan Suderman & Tamara Lush, *Hack Exposes Vulnerability of Cash-Strapped US Water Plants*, AP NEWS (Feb. 2021), https://apnews.com/article/business-water-utilities-florida-coronavirus-pandemic-utilities-e783b0f1ca2af02f19f5a308d44e6abb.

4. Terry Gross & Nicole Perlroth, *U.S. Cyber Weapons Were Leaked – And Are Now Being Used Against Us, Reporter Says*, NAT'L PUB. RADIO: NAT'L SEC. (Feb. 2021), https://www.npr.org/transcripts/966254916.

5. VOA News, *North Korea Hacked Pfizer to Steal COVID-19 Vaccine Data, South Korea Says*, VOA NEWS: COVID-19 PANDEMIC (Feb. 2021), https://www.voanews.com/covid-19-pandemic/north-korea-hacked-pfizer-steal-covid-19-vaccine-data-south-korea-says.

6. Maggie Miller, *Election Commission Approves New Guidelines to Secure, Update Voting Equipment*, THE HILL: POLICY (Feb. 2021), https://thehill.com/policy/cybersecurity/538216-election-commission-approves-new-guidelines-to-secure-update-voting..

7. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, ENERGY SECTOR (Apr. 2021), https://www.cisa.gov/energy-sector.

8. Naylor, *supra* note 1.

9. *Id*.

10. *Id*.

barriers to information-sharing is becoming increasingly important where protecting our nation's critical infrastructure is concerned, particularly within the energy sector.[11]

Order No. 848, promulgated by the Federal Energy Regulatory Commission (FERC) in 2018, augmented the reporting requirements for various types of cyber-attacks on the electric grid[12] and addressed growing concerns about the vulnerability and cybersecurity of the electric grid.[13] Because maintaining a resilient grid is an integral part of the critical infrastructure within the United States,[14] FERC took steps to redefine key terms in the industry and reassess the previously-utilized reporting requirements used by North American Electric Reliability Corporation (NERC) in reporting attacks or breaches of security.[15] FERC also set out new guidelines for addressing both actual and attempted cyber incidents affecting the electric grid.[16]

While the overall costs and benefits of this rulemaking cannot yet be adequately determined,[17] through increasing awareness of threats to the nation's cyber assets, Order No. 848 has the potential to protect the nation from severe economic damage and even prevent human casualties.[18]

II. BACKGROUND

A. Authority and Execution

1. FERC

Through section 215 of the Federal Power Act (FPA), the Energy Policy Act of 2005 gave FERC the authority to certify an electric reliability organization (ERO) to "establish and enforce reliability standards for the bulk-power system, subject to [FERC's] review."[19] FERC had the authority to adopt Order No. 848, pursuant to section 215(d)(5) of the FPA,[20] which further provides that FERC can

11. *See, e.g.*, Office of Elec., *DOE Office of Electricity Issues Request for Information for Bulk-Power System Executive Order*, DEP'T OF ENERGY (July 2020), https://www.energy.gov/oe/articles/doe-office-electricity-issues-request-information-bulk-power-system-executive-order; Securing the U.S. Bulk-Power Sys., 85 Fed. Reg. 41,023 (Dep't of Energy July 8, 2020) (notice for the request for information (RFI)).

12. Order No. 848, *Cyber Security Incident Reporting Reliability Standards*, 164 F.E.R.C. ¶ 61,033, at PP 1-7 (2018) [hereinafter Order No. 848].

13. *Id.*; AM. PUB. POWER ASS'N, SECURITY AND RESILIENCE (CYBER AND PHYSICAL) ISSUE BRIEF: GRID SECURITY (Jan. 2021), https://www.publicpower.org/policy/grid-security.

14. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 7.

15. Order No. 848, *supra* note 12, at PP 1-7.

16. *Id.*

17. *Id.* at PP 29-30.

18. Testimony of the Foundation for Resilient Societies, FERC Reliability Tech. Conference, FERC Docket No. AD17-8-000 (June 22, 2017), https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/thomas_popik_testimony_ferc_technical_conference_june_22_2017_filed__20170619.pdf [hereinafter Popik Testimony].

19. 16 U.S.C. § 824o(a)(2) (2005).

20. Order No. 848, *supra* note 12, at PP 1, 6.

require NERC "to submit to [FERC] a proposed reliability standard or a modification of a reliability standard that addresses a specific matter if [FERC] considers such a new or modified reliability standard appropriate to carry out this section."[21] FERC exercised this power in the promulgation of Order No. 848 because it surmised that the former cybersecurity reporting standards were not sufficiently identifying and classifying potential threats to the bulk electric system (BES).[22]

2. NERC

NERC is the electric reliability organization (ERO) for North America, subject to oversight by FERC.[23] NERC has a number of responsibilities, such as conducting risk management, assessing reliability, monitoring the power grid, and producing the aforementioned reliability standards.[24] The NERC Reliability Standards "define the reliability requirements for planning and operating the North American bulk power system and are developed using a results-based approach that focuses on performance, risk management, and entity capabilities."[25]

NERC implements FERC's regulatory delegation related to cybersecurity pursuant to the Critical Infrastructure Protection (CIP) Standards.[26] The CIP standards establish the minimal criteria required to protect, maintain, and recover the BES and its related critical cyber assets.[27] For context, under NERC's standards, any piece of technology could constitute a "cyber asset" if, within 15 minutes of its dysfunction, it "adversely impact[s] one or more [f]acilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the [BES]."[28] These standards have significantly changed over time, but each of the CIP standards that are directly

21. 16 U.S.C. § 824o(d)(5) (2005).

22. Order No. 848, *supra* note 12, at P 2.

23. NERC, ABOUT NERC (Apr. 2021), https://www.nerc.com/AboutNERC/Pages/default.aspx.

24. *Id.*

25. NERC, STANDARDS (Apr. 2021), https://www.nerc.com/pa/Stand/Pages/Default.aspx.

26. Order No. 706, *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 F.E.R.C. ¶ 61,040, at PP 1-13 (2008) (to be codified at C.F.R. pt. 40) [hereinafter Order No. 706]; *see also*, N. AM. ELEC. RELIABILITY CORP., CIP STANDARDS (Apr. 2021), https://www.nerc.com/pa/Stand/Pages/Default.aspx [hereinafter CIP STANDARDS].

27. Margaret Rouse & Ben Cole, *Definition: NERC CIP (Critical Infrastructure Protection)*, SEARCH COMPLIANCE (July 2012), https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection.

28. N. AM. ELEC. RELIABILITY CORP., LESSON LEARNED CIP VERSION 5 TRANSITION PROGRAM: COMMUNICATIONS TO BES CYBER SYSTEMS AND BES CYBER ASSETS (Nov. 2015).

connected with the topics of focus within[29] are still actively enforced (though some of them have been modified and/or updated).[30]

B. Definitional History and Changes

On July 19, 2018, FERC issued Order No. 848, which expanded upon the mandatory reporting requirements for "cyber security incidents" in NERC's Reliability Standards.[31] Before FERC Order No. 848, a "cyber security incident" was defined by NERC as a "malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter [(ESP)] or Physical Security Perimeter or, disrupts, or was an attempt to disrupt, the operation of a [Bulk Electric System (BES)] Cyber System."[32] "Cyber security incidents" were distinguished from "reportable cyber security incidents" based on whether the attack actually "compromised or disrupted one or more reliability tasks of a functional entity."[33] NERC has since updated its reliability standards to comply with Order No. 848.[34]

After the promulgation of FERC Order No. 848, NERC produced a compliance filing that was ultimately approved by FERC.[35] Some of the relevant changes included the definition of "cyber security incident," which was expanded to include foreign monitoring or breaches of security of the ESPs and Electronic Access Control or Monitoring Systems (EACMS) that were connected with medium

29. Order No. 848, *supra* note 12, at PP 5, 11-12, 54. *See also, e.g.*, N. AM. ELEC. RELIABILITY CORP., CIP-008-5, CIP STANDARD: CYBER SECURITY – INCIDENT REPORTING AND RESPONSE PLANNING (Jul. 2014); N. AM. ELEC. RELIABILITY CORP., CIP-007-6, CIP STANDARD: CYBER SECURITY – SYSTEM SECURITY MANAGEMENT (Jan. 2016); N. AM. ELEC. RELIABILITY CORP., CIP-006-6, CIP STANDARD: CYBER SECURITY – PHYSICAL SECURITY OF BES CYBER SYSTEMS (Jan. 2016); N. AM. ELEC. RELIABILITY CORP., CIP-005-5, CIP STANDARD: CYBER SECURITY – ELECTRONIC SECURITY PERIMETER(S) (Nov. 2013); N. AM. ELEC. RELIABILITY CORP., CIP-002-5, CIP STANDARD: CYBER SECURITY – BES CYBER SYSTEM CATEGORIZATION (Nov. 2012); *see also* N. AM. ELEC. RELIABILITY CORP., CIP-008-6, CIP STANDARD: CYBER SECURITY – INCIDENT REPORTING AND RESPONSE PLANNING (Feb. 2019); N. AM. ELEC. RELIABILITY CORP., CIP-005-7, CIP STANDARD: CYBER SECURITY – ELECTRONIC SECURITY PERIMETER(S) (Nov. 2020); N. AM. ELEC. RELIABILITY CORP., CIP-002-5.1a, CIP STANDARD: CYBER SECURITY – BES CYBER SYSTEM CATEGORIZATION (Dec. 2016).

30. CIP STANDARDS, *supra* note 26.

31. Order No. 848, *supra* note 12, at P 1.

32. NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS, (updated Jan. 2, 2020), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

33. *Id*. "Cyber security incidents" used to include any sort of tampering—which could be as minimal as monitoring—whereas "reportable cyber security incidents" were characterized by whether those cyber events actually accomplished something in terms of disrupting reliability functions of either cyber assets or the BES.

34. NERC, CYBER SECURITY – INCIDENT REPORT TECHNICAL RATIONALE AND JUSTIFICATION FOR RELIABILITY STANDARD CIP-008-6, at 2 (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf.

35. *Letter to Lauren Perotti & Marisa Hecht*, 167 F.E.R.C. ¶ 61,230, at P 1 (Jun. 20, 2019) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Docket%20No.%20RD19-3-000.pdf.

to high impact BES Cyber Systems.[36] This expansion was likely in response to the ever-increasing frequency of foreign interference with cyber assets.[37]

ESPs and EACMSs were not previously protected under the definition of "cyber security incidents" but are now included because they are an integral part of maintaining cyber safety and resilience of the grid. ESPs "manage electronic access to BES Cyber Systems to support the protection of the BES Cyber Systems against compromise that could lead to misoperation or instability."[38] They are "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."[39] Their purpose is to protect cyber assets, like EACMs, and to facilitate remote accessibility.[40]

EACMS "control electronic access to the ESP and play a significant role in the protection of high and medium impact BES Cyber Systems."[41] They can take many forms but are most recognizable for their roles as "firewalls, authentication servers, security event monitoring systems, intrusion detection systems and alerting systems."[42] The Notice of Proposed Rulemaking (NOPR) that proceeded Order No. 848 noted that the ultimate concern is that "once an EACMS is compromised, an attacker could more easily enter the ESP and effectively control the BES Cyber System or Protected Cyber Asset."[43] These modifications are enforced by NERC through its reliability standard, CIP-008-6.[44]

C. Increase in Inter-Agency Communications

On a related note, the final rule that FERC adopted increases the reporting requirements to include entities such as the Department of Homeland Security (DHS).[45] This is significant because it is a clear, measurable move to increase inter-agency communications and minimize security risks. The attacks of Sep-

36. *Id.*

37. Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, SENATE SELECT COMM. ON INTELLIGENCE 5 (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

38. Order No. 848, *supra* note 12, at P 10.

39. NERC, GLOSSARY OF TERMS USED IN NERC RELIABILITY STANDARDS (updated Jan. 2, 2020), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

40. NERC, LESSON LEARNED CIP VERSION 5 TRANSITION PROGRAM: COMMUNICATIONS TO BES CYBER SYSTEMS AND BES CYBER ASSETS (2015).

41. Order No. 848, *supra* note 12, at P 10.

42. *Id.*

43. *Id.*

44. NERC, CYBER SECURITY – INCIDENT REPORT TECHNICAL RATIONALE AND JUSTIFICATION FOR RELIABILITY STANDARD CIP-008-6, at 2 (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf.

45. Order No. 848, *supra* note 12, at P 3.

tember 11, 2001, highlighted some severe failings regarding inter-agency communications.[46] This final rulemaking has pointed out that FERC has the goal of improving "awareness of existing and future cyber threats and potential vulnerabilities"[47] and ultimately, that providing more specific and exhaustive information on cyber incident attempts "will likely better assist the industry in preventing successful cyber-attacks."[48]

D. Order 848

1. Pertinent Language of the Promulgated Rule

This final rulemaking, in short, requires NERC "to develop and submit modification to the NERC Reliability Standards."[49] It states that:

> (1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[50]

E. NERC's Implementation Directed by FERC

To enforce Order No. 848, FERC ordered NERC "to develop and submit Reliability Standard requirements" that met the aforementioned four directives.[51] The first directive is that "responsible entities [must] report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS."[52]

The second requirement is that NERC must "specify the required information in Cyber Security Incident reports."[53] NERC has now implemented this change and deleted confusing requirements from earlier CIP standards and to consolidate them into one rule, R4 of CIP-008-6, in order to satisfy FERC's intentions behind

---

46. 9/11 COMM'N REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, https://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

47. Order No. 848, *supra* note 12, at P 6.

48. *Id.* at P 23.

49. *Id.* at P 1.

50. *Id.* at P 3.

51. *Id.* at P 16.

52. Order No. 848, *supra* note 12, at P 16.

53. *Id.*

Order No. 848.[54] R4 now also addresses the required reportable incident attributes, methods for submitting notifications, notification timing, and notification updates.[55] This rule became effective on January 1, 2021.[56]

Additionally, NERC has "establish[ed] deadlines for filing Cyber Security Incident reports that are commensurate with incident severity."[57] This is an important point in response to some of the concerns expressed by various agencies regarding the burden and usefulness of reporting, which will be discussed later in greater detail. R4 provides for two separate reporting deadlines, one for "reportable" cybersecurity incidents, and the other for more general attempts to compromise systems.[58] Accordingly, reportable cybersecurity deadlines must be reported within an hour, in accordance with CIP-008-5, and NERC provides that attempts to compromise a cyber system must be reported within a calendar day.[59] Correlating the reporting deadline with incident severity is a flexible way in which agencies could more easily accommodate their work load and prioritize their efforts and finite resources.[60]

Finally, Cyber Security Incident reports must "be sent to ICS-CERT, in addition to E-ISAC" and NERC must "file with the Commission an annual, public, and anonymized summary of such reports."[61] In the draft of R4, NERC did not provide for a mandatory method of reporting incidents and instead directed that the relevant entities "focus on incident response itself and not the method or format of reporting," so long as it meets the other requirements under the Reliability Standard.[62]

---

54. NERC, CYBER SECURITY – INCIDENT REPORT TECHNICAL RATIONALE AND JUSTIFICATION FOR RELIABILITY STANDARD CIP-008-6, at 4 (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf; 167 F.E.R.C. ¶ 61,230 Docket No. RD19-3-000 (June 2019), https://cms.ferc.gov/sites/default/files/2020-04/E-2_8.pdf.

55. *Id. See also* current NERC standard CIP-008-6 at; https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-008-6&title=Cyber%20Security%20%E2%80%94%20Incident%20Reporting%20and%20Response%20Planning&Jurisdiction=United%20States.

56. NERC, MANDATORY STANDARDS SUBJECT TO ENFORCEMENT, https://www.nerc.net/standardsreports/standardssummary.aspx# (last visited Apr. 9, 2021).

57. Order No. 848, *supra* note 12, at P 16.

58. NERC, CYBER SECURITY – INCIDENT REPORT TECHNICAL RATIONALE AND JUSTIFICATION FOR RELIABILITY STANDARD CIP-008-6, at 5 (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf.

59. *Id.*

60. Order No. 848, *supra* note 12, at P 52.

61. *Id.* at P 16.

62. NERC, CYBER SECURITY – INCIDENT REPORT TECHNICAL RATIONALE AND JUSTIFICATION FOR RELIABILITY STANDARD CIP-008-6, at 5 (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf.

Before this change, Cyber Security Incidents were reported under NERC's Reliability Standard CIP-008-5.[63] This standard is different from the proposal because it only required that an entity report incidents that actually managed to "compromise[] or disrupt[] one or more reliability tasks."[64] FERC explained that this reporting standard did not accurately depict "the true scope of cyber-related threats facing the [BES]" and that many cyber-attacks, or attempted cyber-attacks, were not meeting the minimum criteria to require reporting.[65] One of the main pieces of evidence to support FERC's conclusion was the fact that there were no reportable cybersecurity incidents during 2015 and 2016, meaning that no attacks resulted in a loss of load.[66] NERC, in a Reliability Report on the subject, noted that the lack of reportable incidents did not necessarily mean that there was a low or minimal risk of cybersecurity incidents.[67]

F. Policy of the Order

The NOPR set three (3) minimum attributes that should be used when reporting incidents, so as to "improve awareness of cyber threats to BES reliability."[68] The first is to include the achieved or *attempted* functional impact of the Cyber Security Incident.[69] The second mandates that "the attack vector used to attempt or achieve the Cyber Security Incident" be included.[70] The final suggested attribute goes to "the level of intrusion achieved or attempted by the Cyber Security Incident."[71]

1. Comments

One of the major concerns highlighted from the comments to the NOPR was whether or not augmenting the reliability standard would unduly burden the industry.[72] NERC agreed with increasing the reporting requirements under the NOPR and provided that it would "help enhance awareness of cyber security risks facing entities" and that it "would create a more extensive baseline understanding the nature of cyber security threats and vulnerabilities."[73] This is consistent with the goal NERC provided in its 2017 State of Reliability Report as well.[74] NERC, however, did not support the NOPR regarding enhancing reporting requirements through a Reliability Standard.[75]

---

63. Notice of Proposed Rulemaking, *Cyber Security Incident Reporting Reliability Standards,* 82 Fed. Reg. 61,499 (Dec. 28, 2017), 161 F.E.R.C. ¶ 61,291, at P 1 (2017).

64. Order No. 848, *supra* note 12, at P 2.

65. *Id.*

66. *Id.* at P 9.

67. *Id.*

68. *Id.* at P 13.

69. Order No. 848, *supra* note 12, at P 13.

70. *Id.*

71. *Id*.

72. *Id.* at PP 22-30.

73. *Id*. at P 22.

74. Order No. 848, *supra* note 12, at P 22.

75. *Id*.

There were many supporters of broadening the definition of "Reportable Cyber Security Incidents" on the policy grounds that having better definitions would help prevent cyberattacks.[76] These supporters did have some worries and suggestions.[77] Some of the supporting entities believed that there was a "risk of over-reporting," that reporting attempts regarding "an ESP or associated EACMS 'needs further clarification,'" that some of the information reported might not be useful, and that there should be further guidance on what constitutes an "attempt."[78]

2. Outcome

FERC ultimately adopted the NOPR proposal, agreeing with NERC and other commenters "that enhanced reporting of Cyber Security Incidents will address an existing gap in Cyber Security Incident reporting and will provide useful information on existing and future cyber security risks, as well as provide entities with better visibility into malicious activity prior to an event occurring."[79] There were also some concerns that the new reporting requirements could divert resources away from other important programs.[80] FERC rejected this position because "responsible entities are already required to monitor and log successful login attempts, detected failed access attempts, and failed login attempts under Reliability Standard CIP-007-6, Requirement R4.1."[81]

Worries were also expressed regarding the minimum requirement for reporting a Cyber Security Incident.[82] Commenters repeated their concerns about the burden of setting certain threshold reporting requirements, but FERC ultimately decided to set a "compromise or attempted compromise of an ESP as the appropriate threshold for a Reportable Cyber Incident."[83] FERC agreed with several of the comments regarding the need for building flexibility into the reporting standard, and it suggested a system that reflects the severity of the incident with its reporting deadlines.[84]

G. Significance in the United States

BES disturbances are a matter of national security with potentially dire consequences, as can be seen with the blackout that occurred in Ukraine in December of 2015.[85] The Ukraine cyber-attack cut off the power going to 225,000 people in

76. Order No. 848, *supra* note 12, at P 23.

77. *Id*.

78. *Id.*

79. *Id.* at P 31.

80. *Id.* at P 33.

81. Order No. 848, *supra* note 12, at P 34.

82. *Id.* at PP 34-51.

83. *Id.* at P 52.

84. *Id.*

85. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [hereinafter Zetter, *Inside the Hack of Ukraine's Power Grid*].

western Ukraine, depriving them of critical heating in the harsh winter months.[86] The Ukraine attack was described as "a premeditated and multi-level invasion," but one that was "not meant to be large scale."[87] Even several months after that infamous attack, power providers were still having difficulties maintaining stability and returning to normal usage.[88]

Since the Ukraine attack and others like it, the Pentagon has conducted tests to determine what could happen in a worst-case-scenario attack on the United States power grid.[89] Researchers simulated what it would be like for the power grid to be inoperable and what measures it would take to resume reliable operation.[90] The study showcased how difficult that task can be and what effects a large-scale blackout could have on the United States.[91] For instance, government or military officials might have to pick and choose which critical assets (such as hospitals and military bases) to provide power to during an event.[92] Or, for example, following a nuclear terrorist attack, power would be most important to first-responders and military officials.[93] The unique interdependencies of critical infrastructure within the United States today can "expose new vulnerabilities" when faced with terrorism or other interruptions.[94] Thus, communication between governmental actors and the private sector becomes crucial for stabilization.[95]

The first notable cyber-attack on the United States power grid occurred on March 5, 2019.[96] Luckily, this attack did not result in any blackouts or harm power generation, although it did have some slight effect on the Western transmission grid.[97] A director of intelligence analysis at a cybersecurity firm notes that the power grid touches nearly every part of a modern North American's day and that "many other critical infrastructure sectors rely on electricity."[98]

---

86. Pavel Polityuk, Oleg Vukmanovic & Stephen Jewkes, *Ukraine's Power Outage Was a Cyber Attack: Ukrenergo*, REUTERS (Jan. 18, 2017), https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA.

87. Order No. 848, *supra* note 12, at P 52.

88. Zetter, *Inside the Hack of Ukraine's Power Grid*, *supra* note 85.

89. Joseph Marks, *Pentagon Researchers Test 'Worst-Case Scenario' Attack on US Power Grid*, DEFENSE ONE (Nov. 14, 2018), https://www.defenseone.com/technology/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152829/?oref=d-channelriver.

90. *Id.*

91. *Id*.

92. *Id.*

93. *Id*.

94. Randy Atkins, *Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop*, NAT'L ACAD. PRESS (2006), https://www.nap.edu/read/11698/chapter/6.

95. *Id*.

96. Blake Sobczak, *Experts assess damage after first cyberattack on U.S. grid*, E&E NEWS (May 6, 2019), https://www.eenews.net/stories/1060281821.

97. *Id.*

98. *Id.*

III. ANALYSIS

A. Overview

Due to the lack of cybersecurity incidents reported in 2015-2016, FERC explained that cyber-attacks or incidents were not meeting the defined criteria to make those attempts reportable in nature.[99] NERC pointed out that a lack of reportable incidents does not necessarily indicate that there is no cause for concern; lower-level attacks and data collection from hackers could occur but not trigger the requirement to report.[100] Because of this, FERC adopted Order No. 848 to increase reporting requirements and to clarify definitions and boundaries for reporting incidents.[101] Order No. 848's augmentation of reporting requirements is intended to increase inter-agency communication, the degree and type of information collected pertaining to potential cybersecurity grid threats, the awareness and consciousness of risks involving the grid, and ultimately increase national security.[102]

B. Effectiveness

1. Methodology

The main point of Order No. 848 is to increase the reporting requirements for cybersecurity incidents so that there is more information on what types of threats hackers pose and to ultimately protect the BES from harm.[103] To accomplish this, FERC ordered that NERC modify the existing Reliability Standards and develop further protocols consistent with the Order.[104] The increase in mandates also augmented inter-agency communication.[105]

2. Implementation

Following the issuance of Order No. 848, NERC published an Implementation Guide detailing the Reliability Standards to be changed and providing more specific guidelines for mandated reporting.[106] NERC also provided a cyber security incident reporting form, which included categories such as attack vector, functional impact, and level of intrusion, to ensure consistency in their reports.[107] NERC directed the Responsible Entities[108] to "determine what is normal within

99. Order No. 848, *supra* note 12, at P 9.

100. *Id*.

101. *Id.*

102. *Id.* at PP 13, 22-23.

103. Order No. 848, *supra* note 12, at PP 1-4.

104. *Id.* at PP 1-2, 31.

105. *Id.* at P 34.

106. NERC, CYBER SECURITY – INCIDENT REPORTING AND RESPONSE PLANNING IMPLEMENTATION GUIDANCE FOR CIP-008-6, at 4 (2019) [hereinafter NERC Implementation Guide].

107. *Id.* at 43.

108. Responsible Entities include, for example, Standards Developers, Transmission Planners, Reliability Assurers, Market Operators, and other entities that perform reliability functions. NERC's reliability standards are mandatory for Responsible Entities. NERC, RELIABILITY FUNCTIONAL MODEL FUNCTION DEFINITIONS AND

their environment to help scope and define what constitutes 'an attempt to compromise'" the BES, and also to be creative and search for flexible solutions to reduce the burden placed on them.[109] This approach offers a more effective long-term solution to the issue of cybersecurity in the energy sector as a whole, since the Responsible Entities are most able to assess what constitutes "normal" in each of their respective domains.[110]

One potential issue with the language in the aforementioned directive is that it has the potential to undermine the purpose of Order No. 848 entirely, which is to address the lower-level potential threats that the entities are not catching.[111] For example, an entity could determine that a low-level threat is not outside of the range of every day activity. However, after months of low-level data gathering, hackers could use the collected data to launch a strategic, highly-specific attack.[112] The entity, in this hypothetical, would have simply passed on its opportunity to prevent the harmful attack because it deemed an earlier event to be within normal activity levels. Such was the case with the 2015 Ukraine attack.[113] Thus, the language of this directive must be carefully scrutinized to provide viable solution to preventing overly burdensome agency reporting.

3. Risks of the Order

a. Critiques

As noted earlier, during the Notice and Comment period, there were some critiques posed by various agencies and private entities arguing that implementation of the NOPR would unduly burden the agency and divert voluntary reporting resources.[114] For example, while Eversource and Idaho Power admitted that implementation of the proposal could "provide some visibility into the types of threats that [energy providers] face," the augmentation of reporting requirements would "reduce the finite resources that [energy providers] have to monitor and defend their critical infrastructure."[115]

Several comments also addressed the need for Order No. 848 to define an "attempt" to compromise the system and to specify the types of assets the Responsible Entities needed to monitor, rather than promulgating broad demands.[116] These arguments were made in the interest of not overburdening agencies with

---

RESPONSIBLE ENTITIES VERSION 5.1 (Dec. 12 2018), https://www.nerc.com/pa/Stand/Functional%20Model%20Advisory%20Group%20DL/Functional_Model_V5.1_clean_10082019.pdf.

109. NERC Implementation Guide, *supra* note 106, at 20.

110. *Id.*

111. Order No. 848, *supra* note 12, at P 9.

112. Kim Zetter, *Everything We Know About Ukraine's Power Plant Hack*, WIRED (Jan. 20, 2016), https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ [hereinafter Zetter, *Everything We Know*].

113. *Id*.

114. Order No. 848, *supra* note 12, at PP 32-34, 44.

115. *Id.* at P 29.

116. *Id.* at P 52.

inefficient, redundant, or unhelpful reports.[117] These critiques are supported by Andrea Matwyshyn in her law review article focused on the shortcomings of the legal system in regards to cybersecurity.[118] Matwyshyn recognizes the severity of a breach of cybersecurity in both the public and private sectors but says that the two major legal paradigms surrounding cybersecurity are insufficient, as they are.[119] Notably, Matwyshyn points out that these paradigms do not address the underlying issues regarding the cause of cyber attacks and can lead to a focus on information sharing rather than paying attention to the actual substance of the obtained information.[120]

Another major critique of Order No. 848 was that it was overly broad and that it would not adequately address the gaps in the reporting of cyber security incidents.[121] For example, an intervenor group, Trade Associations, argued that the broad language of Order No. 848 could actually lead to a reduction in awareness of *significant* cyber threats (i.e., ones that do more than just attempt to compromise ESPs or EACMS).[122]

b. FERC's Direct Response to Critiques

In response to these critiques, FERC pointed out that its purpose was neither to unduly burden agencies and private entities nor to prescribe overly broad mandates, but that it was trying to support NERC's development of adequate and flexible standards for the industry.[123] Further, NERC also indicated that it would work to make sure that the reporting requirements were flexible and not "unduly burdensome" for the affected entities.[124]

4. Benefits of the Order

To truly understand the benefits of the Order, the severity and consequences of a potential, severe blackout must be addressed. Security of the BES is intensely important as each economic sector, making up the critical infrastructure of the nation, relies on having a resilient electric grid.[125] In 2017, Thomas Popik, the Foundation for Resilient Societies' founder and chairman,[126] testified before FERC to detail what exactly a long-term, large-scale blackout would look like in the United States.[127] A long-term and large-scale blackout is one that "[p]ersists

117. *Id.* at P 63.

118. Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109 (2017).

119. *Id.* at 1124-25.

120. *Id.* at 1128.

121. Order No. 848, *supra* note 12, at P 33.

122. *Id.* at PP 44, 49. The Trade Associations is made up of: American Public Power Association, Electricity Consumers Resource Council and Transmission Access Policy Study Group.

123. *Id*. at P 32.

124. *Id*.

125. Robert Knake, *A Cyberattack on the U.S. Power Grid*, COUNCIL ON FOREIGN RELATIONS (Apr. 2017), https://www.jstor.org/stable/resrep05652.

126. Thomas Popik, *Our Energy Policy*, https://www.ourenergypolicy.org/author/thomaspresilientsocieties-org/.

127. Popik Testimony, *supra* note 18.

longer than the supplies of backup energy necessary for grid restoration" and "[c]overs a geographic area so large that significant outside assistance is impractical."[128]

Luckily, the United States has never experienced a blackout that would meet such criteria, as most of the major blackouts in the United States have been resolved within twenty-four (24) hours.[129] A long-term and large scale blackout could lead to devastating consequences in our nation.[130] Within two (2) minutes of the BES failing, affected nuclear power plants would have to turn on emergency diesel generators since the Nuclear Regulatory Commission (NRC) requires the grid to be stable in order for nuclear plants to operate.[131] This measure is to cool the plants down, not to produce more energy.[132] Sixteen (16) hours into the blackout, most telecommunication functions would be inoperable, with the exception of the few offices that have a seventy-two (72) hour backup fuel supply.[133] Within a few days, vehicles that ran out of fuel would clutter the streets, government services would stop, critical infrastructure would be damaged or destroyed entirely, and human casualties could potentially reach the millions.[134] Additionally, the backup diesel generators at the nuclear plant would likely have run out by the seventh day which would cause the reactor cores to overheat and the spent fuel pools to boil.[135] Without any change in the conditions, by the 30th day, nuclear plants will have become highly radioactive and unsafe for humans to be around.[136] Further, there is a likelihood that some fuel pools would ignite, which could create "plumes of radioactive material over large areas."[137]

Although the United States has not experienced a large-scale, long-term blackout, the consequences from some of the major blackouts in the United States still present a cause for concern.[138] For example, in 2003, the Northeast Blackout left about fifty million (50,000,000) individuals without power.[139] This blackout resulted in four (4) to ten (10) billion dollars in economic loss, even though the majority of this event did not last for more than a day.[140] At large, the United States is estimated to have lost between twenty (20) to fifty-five (55) billion dollars due *specifically* to power outages related to the weather.[141] As a recent example,

128. *Id*. at P 1.
129. *Id.*
130. *Id.*
131. Popik Testimony, *supra* note 18, at P 2.
132. *Id*.
133. *Id.*
134. *Id.* at P 1.
135. Popik Testimony, *supra* note 18, at P 2.
136. *Id.*
137. *Id.*
138. *Id.* at P 1; Knake, *supra* note 125, at 3.
139. Knake, *supra* note 125, at 3.
140. *Id.* at 3; Popik Testimony, *supra* note 18, at 1; Chris Bronk, *Hacks on Gas: Energy, Cyber Security, and U.S. Defense*, STRATEGIC STUDIES INST., US ARMY WAR COLLEGE, at 303 (2015).
141. Salahuddin Qazi, *Power Outage*, Photovoltaics for Disaster Relief and Remote Areas (2017), https://www.sciencedirect.com/topics/engineering/power-outage.

Winter Storm Uri caused ERCOT to order rolling blackouts "to keep the grid from shutting down altogether."[142] To date, costs of Winter Storm Uri are still being calculated; some estimate costs could be as much as $200 billion[143] while it cost dozens of individuals their lives.[144] ERCOT CEO, Bill Magness, spoke out on the matter and explained that the rolling blackouts were necessary "to prevent a widespread blackout that could last months" or longer.[145] Although the United States has not experienced a long-term, large-scale blackout, an event of that severity would almost certainly result in severe economic loss (in the billions) and drastic damage to the critical infrastructure of the country.[146] Protecting the BES is necessary because a successful cyber-terrorist attack on the grid could leave the nation devastated and in shambles.

The severity of a successful attack is precisely why augmenting the reporting requirements is so important; such a move is warranted in spite of critiques for a number of reasons. The majority of the critiques received were concerned with the burdens that the new reporting requirements might cause or concerned that unhelpful data would be reported. FERC essentially conducted a cost-benefit analysis and determined that the increased burden would be worth the potential benefits in this area. Some scholars have concluded that the cost of compliance with the NERC Reliability Standards is questionable, although these conclusions fail to take into account more modern economic trends and technologies.[147] Other analyses take into account the initial responses from Responsible Entities and highlight the acceptance process that comes along with imposing new regulations.[148] The Responsible Entities failed to provide a detailed explanation or quantify costs for compliance regarding the ways in which complying with Order No. 848 would overburden them.[149] Additionally, the cost of the increase in reporting can be budgeted for by grid operators;[150] this cost can be estimated and planned for

142. Jan Wesner Childs, *Why Winter Storm Uri Caused Millions of Power Outages in Texas*, WEATHER CHANNEL (Feb. 16, 2021), https://weather.com/news/news/2021-02-16-why-so-many-power-outages-in-texas-winter-storm.

143. Irina Ivanova, *Texas winter storm could top $200 billion – more than hurricanes Harvey and Ike*, CBS NEWS (Feb. 25, 2021), https://www.cbsnews.com/news/texas-winter-storm-uri-costs/.

144. Reis Thebault, Paulina Firozi & Brittany Shammas, *58 people died in last week's frigid weather. Some of them were just trying to stay warm*., WASHINGTON POST (Feb. 21, 2021), https://www.washingtonpost.com/nation/2021/02/18/winter-storm-deaths/.

145. Christian Flores, *CEO of ERCOT says rolling outages were necessary to prevent widespread blackout*, CBS AUSTIN (Feb. 17, 2021). https://cbsaustin.com/news/local/ercot-holding-conference-call-on-widespread-outages-affecting-millions-of-texans.

146. Knake, *supra* note 125; Popik Testimony, *supra* note 18; Bronk, *supra* note 140; Qazi, *supra* note 141.

147. William F. Watson, *NERC mandatory reliability standards: A 10-year assessment*, 20 ELEC. J. 9-14 (Feb. 16, 2017).

148. James Stanton, *Where Are We After 10 Years of Bulk Electric System Reliability Standards?*, POWER (Feb. 1, 2017) https://www.powermag.com/where-are-we-after-10-years-of-bulk-electric-system-reliability-standards/.

149. Order No. 848, *supra* note 12, at P 54.

150. NERC, 2019 BUSINESS PLAN AND BUDGET, at 17 (Aug. 8, 2018), https://www.nerc.com/gov/bot/FINANCE/19BusPlanBud/2019%20NERC%20Business%20Plan%20and%20Budget%20-%20Revised%20Final.pdf.

whereas the costs of a significant attack on the grid are completely unknown. The costs for complying with the reliability standards can be passed through to customers on a level basis over time.[151]

Order No. 848 and NERC's Implementation Guide fit into the well-known Swiss Cheese model discussed by James Reason, an author and professor of psychology.[152] Reason describes functional systems to have layers of defenses, barriers, and safeguards to protect the entity in question from various hazards.[153] Safeguards include layers of security that can be provided through utilizing a number of different methods such as data encryption, firewalls, passwords, biometrics, and antivirus.[154] There are, unfortunately, innate holes in those protective technological guards.[155] Those holes often open, shut, and change locations, which can make diagnosing and curing the protective shields' shortcomings rather difficult.[156]

By augmenting the reporting requirements, FERC is effectively trying to address the holes in the protective shields of the BES and to better understand what attackers are looking for, what they are doing, and how to best address those concerns.[157] Although agencies will have more work and procedures to follow, FERC believes that compliance with Order No. 848 does not present agencies with a greater burden than a compromise in the BES would provide.[158] NERC follows the same rationale in its Implementation Guide by encouraging agencies that deal with EACMS and EAPs to change the provided configuration "in favor of architectures that offer layers of safeguards and a defense in depth."[159] This mitigation of risks exemplifies forward and conscious thinking, which should help prevent major large-scale attacks on the grid.

5. Continuing Development

In late 2020, FERC issued a new Notice of Proposed Rulemaking to examine ways to "provid[e] significant cybersecurity benefits for actions taken that exceed the requirements of the CIP Reliability Standards" in order to encourage utility providers to improve and invest in cybersecurity voluntarily; the Cybersecurity Incentives NOPR.[160] Since the CIP Reliability Standards provide a results-based mandate, FERC opined that incentivizing public utility providers to innovate and "to adopt best practices" would help "to protect its own transmission system as

151. *Cybersecurity Incentives, Notice of Proposed Rulemaking,* 173 F.E.R.C. ¶ 61,240, at PP 40–46 (2020).

152. James Reason, *Human Error: Models and Management*, 320 BRITISH MED. J., No. 7237 (Mar. 18, 2000), https://www.jstor.org/stable/25187420.

153. *Id*. at 769.

154. Paul Zandbergen, *System Security: Firewalls, Encryption, Passwords & Biometrics*, STUDY, https://study.com/academy/lesson/systems-security-firewalls-encryption-passwords-biometrics.html.

155. Reason, *supra* note 152.

156. *Id.*

157. Order No. 848, *supra* note 12.

158. *Id.* at P 66.

159. NERC Implementation Guide, *supra* note 106, at 20.

160. Notice of Proposed Rulemaking, *Cybersecurity Incentives*, 173 F.E.R.C. ¶ 61,240, 86 *Fed. Reg.* 8,309 (2021).

well as improve the security of the BES."[161] If the implemented improvements were found to be particularly helpful, they might become mandatory in CIP Reliability Standards later on.[162]

Qualifying for FERC's proposed incentives will not pose an insignificant hurdle; routine improvements and costs associated with CIP Reliability Standard compliance would not make utility companies eligible for FERC's proposed incentives.[163] To qualify for FERC's proposed incentives, the cybersecurity investments must go "above and beyond the requirements of the CIP Reliability Standards, and materially enhance the cybersecurity posture of the Bulk-Power System by enhancing applicant's cybersecurity posture substantially above levels required by the CIP Reliability Standards, to the benefit of ratepayers."[164] FERC took note of its need to establish methods to assess implemented improvements.[165]

FERC wanted to incentivize public utilities to invest in and improve their cybersecurity, largely in response to the COVID-19 pandemic.[166] FERC is acutely aware of the increase in threats and vulnerabilities that come with working from home and the infrastructure necessary to operate the global supply chain.[167] Although there are methods of monitoring cyberthreats in place, FERC recognized their limitations and wanted to induce the implementation of flexible innovations to respond to the ever changing threats the BES faces.[168] It is important to note that the CIP Reliability Standards remain mandatory and effective measures for monitoring and managing cybersecurity threats.[169] However, not all utility providers are required to adhere to the CIP Reliability Standards; the CIP Reliability Standards are mandatory for Responsible Entities[170] to follow.[171] Should the Cybersecurity Incentives NOPR become a final order, it could encourage some providers to voluntarily comply with the CIP Reliability Standards and stimulate cybersecurity improvements within their available means for all utility providers.[172] A final order based on the Cybersecurity Incentives NOPR could also facilitate more efficient and effective response to threats, as creating new Reliability Standards can take months to become operational and enforceable.[173]

---

161. *Id.* at P 14.

162. *Id*.

163. *Id.* at P 3.

164. *Id.* at PP 1, 3.

165. 173 F.E.R.C. ¶ 61,240, at P 15.

166. *Id.* at P 17.

167. *Id*. *See also Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 F.E.R.C. ¶ 61,020 (2018); Letter Order Accepting Proposed Supply Chain Reliability Standards Mandated by Order No. 850, 174 F.E.R.C. ¶ 61,193 (2021).

168. *Id*.

169. *Id*. at P 18.

170. *See supra* note 108.

171. Order No. 848, *supra* note 12, at P 18.

172. *Id*.

173. *Id*. While the formal commenting process at the Commission is not yet complete as of this writing, comments both for and against are expected based on prior statements of interested parties. *See* https://www.utilitydive.com/news/energy-sector-divided-over-transmission-incentives-for-voluntary-cybersecur/584019/. Any

IV. CONCLUSION

In sum, Order No. 848 was promulgated to augment the mandatory reporting guidelines and delegated to NERC to draft a new Reliability Standard.[174] Although Order No. 848 amended the definitions of several key terms within the cybersecurity sphere, there are still concerns as to whether these changes were specific enough to warrant the change.[175] FERC ultimately adopted the NOPR, in spite of complaints that Order No. 848 would be too burdensome on already-spread-thin reporting entities and that the products of their work might not actually be helpful.[176]

The rationale for FERC's decision can be demonstrated through a number of studies and actual cyber-attacks.[177] These studies indicate that a major blackout in the United States would cost a tremendous amount of money, eat up resources, destroy critical infrastructure, potentially leave the country more vulnerable to terrorism, and even possibly lead to millions of human casualties.[178] While Order No. 848 does create more work for reporting entities, the goal of the Order is to help the energy sector better understand what threats lie in wait, bulk-up their protections of Cyber Assets, understand where their systems are vulnerable, and to preserve the resilience of the grid.[179] Adding additional entities and governmental agencies, such as DHS, into the reporting requirements increases inter-agency communications which help to better understand and minimize national security risks.[180] With potentially catastrophic consequences at stake, the benefits of Order No. 848 outweigh the disadvantages.

Shelby Fields[*]

---

final rule will be noteworthy for how comments opposing the NOPR are discussed with respect to issues regarding the cost benefit analysis of the new regulations.

174. Order No. 848, *supra* note 12, at P 1.

175. *Id.* at PP 9, 63.

176. *Id.* at PP 52, 63.

177. Popik Testimony, *supra* note 18; Zetter, *Inside the Hack of Ukraine's Power Grid*, *supra* note 85; Zetter, *Everything We Know*, *supra* note 112; Knake, *supra* note 125; Bronk, *supra* note 140; Qazi, *supra* note 141.

178. Popik Testimony, *supra* note 18.

179. Order No. 848, *supra* note 12, at PP 20, 32.

180. *The 9/11 Commission Report Final Report of the National Commission on Terrorist Attacks Upon the United States*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., https://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

* Shelby Fields is a third-year law student at the University of Tulsa College of Law. She would like to thank Mr. Alex Goldberg, Ms. Delia Patterson, Mr. Jack Cashin, Ms. Shari Gribbon, Professor Warigia Bowman, Professor Ido Kilovaty, Professor Robert Butkin, and the *Energy Law Journal* student and staff editors for all of their hard work and support throughout this process. Fields would also like to thank her colleagues, friends, and family members, particularly her mother and husband, for their unwavering support.