PIPE DREAMS: STREAMLINING CYBERSECURITY REGULATORY AUTHORITY OVER THE ENERGY INDUSTRY TO INCREASE NATIONAL SECURITY

KATHERINE SAUTER*

* J.D. Candidate, 2021, American University Washington College of Law; B.A., Elon University, 2014. I would like to thank Professor Michael Panfil for his invaluable feedback and the staff of the *Administrative Law Review* for their editing assistance. I would also like to thank Professor Elizabeth Keith and Erin Downey for their instruction and mentorship. Finally, I am incredibly grateful to my husband, my family, and Tina Fey for their support and encouragement.

INTRODUCTION

On a Tuesday afternoon on a hot July day, the corporate park you work in loses power, and you are let out early from your nine-to-five job. You appreciate the afternoon off, even if it is only a temporary respite from the weekly routine. You happily drive home, counting the ways you will take advantage of your open evening. You flip through Twitter before running errands and the breaking news changes everything. What was going to be a grocery run will now be an emergency preparedness run; what was an afternoon off may now be an exercise in survival with no end in sight. In a moment, a geographically distributed cyberattack on the nation's natural gas pipeline system causes the electric grid to fail and forces an unprecedented electricity blackout.

Cybersecurity of the nation's critical infrastructure is a priority for federal agencies;[1] however, the approach to reducing cybersecurity vulnerabilities in the energy industry is fragmented and inefficient.[2] While the electricity sector is subject to mandatory cybersecurity standards, natural gas pipelines are offered only voluntary guidelines to better secure those critical infrastructures.[3]

---

1. *See* Exec. Order No. 13,800, 82 Fed. Reg. 22,391, 22,393 (May 11, 2017) (declaring the Executive Branch's policy for strengthening the cybersecurity of the country's critical infrastructure); Directive on Critical Infrastucture and Security, 1 PUB. PAPERS 106, 107–08 (Feb. 12, 2013) [hereinafter Security and Resilience Directive] (expanding national critical infrastructure protection to include a focus on protection from cyber incidents); *see also* Memorandum from the White House, Presidential Decision Directive/NSC-63: Critical Infrastructure Protection 10 (May 22, 1998), https://fas.org/irp/offdocs/pdd/pdd-63.pdf (establishing critical infrastructure sectors). The most recent Presidential Policy Directive listed the sixteen critical infrastructure sectors as: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems. Security and Resilience Directive, *supra*, at 114–115.

2. *See infra* Part II (describing several federal agencies' authority to regulate, provide guidelines, or ensure compliance in the energy industry).

3. *See* Aaron Larson, *FERC and Cybersecurity: It's Complicated*, POWER MAG. (Feb. 28, 2019), https://www.powermag.com/ferc-and-cybersecurity-its-complicated-podcast/ (reviewing differences in cybersecurity regulation between the electricity and natural gas sectors).

In part, this absence of mandatory pipeline cybersecurity standards can be attributed to a jigsaw of federal agencies staking a claim in pipeline oversight.[4]

The Transportation Security Administration (TSA), the federal agency ultimately responsible for pipeline cybersecurity,[5] is not equipped—in resources or industry expertise—to ensure the security of the nation's energy.[6] Since at least 2018, the Federal Energy Regulatory Commission (Commission or FERC)—which approves the mandatory standards in the electricity sector—has unsuccessfuly suggested that Congress move pipeline cybersecurity responsibility to an agency that specializes in energy, such as the Department of Energy (DOE).[7] Some FERC Commissioners are concerned the TSA cannot adequately mitigate the risks of cyber threats.[8] Other Commissioners find voluntary pipeline cybersecurity standards inadequate and recommend implementing mandatory standards,[9] which would parallel the binding regulations in the electricity sector.[10]

Is bifurcated cybersecurity authority over the energy sector still in the nation's best interest?[11] Given the FERC's industry expertise, it should

---

4. *Infra* Part II.

5. *See, e.g.*, PAUL W. PARFOMAK, CONG. RSCH. SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY 1 (2012), https://crsreports.congress.gov/product/pdf/R/R42660 ("The Transportation Security Administration (TSA) is authorized by federal statute to promulgate pipeline physical security and cybersecurity regulations . . . .").

6. *See* Maya Weber, *FERC Commissioners Add to Calls for Cybersecurity Standards for Pipelines*, S&P GLOB. MKT. INTEL. (June 13, 2019), https://www.spglobal.com/marketintelligence/en/news-insights/trending/j9h-0T-B3MAzb9EXDbVymg2 (reporting that this is not TSA's "bailiwick"). Several of the highest-ranking members of the Federal Energy Regulatory Commission (Commission or FERC) find TSA ill-equipped to regulate pipeline cybersecurity. *Id.*

7. *See id.* (noting that Commissioners Glick and LaFleur petitioned for review of pipeline cybersecurity authority).

8. *See id.* (Commissioner Glick's position).

9. *See id.* (former Commissioner LaFleur's position).

10. Lawrence R. Greenfield, *An Overview of the Federal Energy Regulatory Commission and Federal Regulation of Public Utilities*, FERC 7 (June 2018), https://www.ferc.gov/sites/default/files/2020-07/ferc101.pdf.

11. *See* U.S. DEP'T OF ENERGY, STAFF REPORT TO THE SECRETARY ON ELECTRICITY MARKETS AND RELIABILITY 92 (2017), https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf (writing to then-Department of Energy Secretary Perry, North American Electric Reliability Corporation (NERC) CEO, Gerry Cauley, recommended coordinating plans, operations, and regulatory partnerships between the natural gas and electricity sectors, which are so closely interconnected); Mark Rockwell, *TSA's Role in Pipeline Cybersecurity Could Be Up for Grabs*, FCW (Sept. 27, 2018), https://fcw.com/articles/2018/09/27/tsa-pipeline-cyber-rockwell.aspx (describing the objection to voluntary standards for pipelines but mandatory standards for electricity, and that the increasingly connected sectors present a unique vulnerability); *see also*

have authority over mandatory cybersecurity regulations for both the electricity and natural gas pipeline sectors. This Comment argues that the FERC should reinterpret its scope of authority under the Natural Gas Act (NGA) and regulate natural gas pipeline cybersecurity standards. Additionally, this Comment suggests limiting the TSA's pipeline authority to physical security.

Part I briefly overviews the energy industry and highlights the important relationship between electricity and natural gas, and the unique cyber vulnerabilities this relationship creates. Part II focuses on the many federal agencies and offices with some cybersecurity responsibility for the electricity sector and interstate natural gas pipelines. Part III briefly outlines current cyber standards that mitigate risk in the electricity and natural gas sectors. Finally, Part IV recommends an integrated approach to better protect the energy industry as a whole and streamline federal regulatory authority. This integrated approach grants the Commission with natural gas pipeline cybersecurity authority and suggests creating mandatory standards for pipelines. Additionally, the Commission should create a natural gas pipeline reliability organization that would oversee the development, adoption, and enforcement of the mandatory standards.

I. AN OVERVIEW OF THE ENERGY INDUSTRY

A. The Energy Industry

Energy resources are the building blocks of the energy industry and provide the groundwork for the forms of energy we use every day. In the United States, available energy resources include fossil fuels (coal, oil, and natural gas), nuclear power, and renewable resources (hydropower, wind, solar, biomass and geothermal energy).[12] These energy resources are either converted into electricity, used in transportation, or used by industrial, commercial, or residential consumers.[13]

Built on the foundation of energy resources, the U.S. energy industry is comprised of three interrelated sectors: electricity, natural gas, and oil.[14]

---

infra Parts I.B, II.B (explaining the separation between electricity and natural gas in the energy industry, and in the Commission's regulatory authority).

12. JOEL B. EISEN ET AL., ENERGY, ECONOMICS AND THE ENVIRONMENT: CASES AND MATERIALS 2 (4th ed. 2015).

13. *See id.*

14. U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF ENERGY, ENERGY SECTOR-SPECIFIC PLAN 2 (2015) [hereinafter ENERGY PLAN], https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. The oil sector is critical to the nation's energy economy, with oil products accounting for 92% of all transportation fuels consumed in the

This Comment focuses on the electricity and natural gas sectors, and will discuss each in turn. The electricity sector is typically divided into three functions: (1) generation and storage; (2) transmission; and (3) distribution.[15] Generating resources and high-voltage transmission lines together creates the bulk power system.[16] High-voltage power transmission, often collectively referred to as the "grid," is comprised of three interconnected electric transmission systems that together form a nationwide system that enables (for example) lights to turn on and cell phones to charge.[17] Because large quantities of electricity cannot be stored easily or effectively, grid operators must expertly balance power generation and transmission—or the supply and demand of electricity—at all times to prevent a blackout.[18]

Like the electric industry, the natural gas industry historically encompasses three sectors: (1) upstream natural gas production, gathering, and processing; (2) pipeline transportation and storage; and (3) local distribution.[19] Surprisingly, each sector is subject to different regulatory oversight.[20]

United States in 2014. FERC, ENERGY PRIMER: A HANDBOOK OF ENERGY MARKET BASICS 103 (2015), https://www.ferc.gov/market-assessments/guide/energy-primer.pdf [http://web.archive.org/web/20200512020101/https://ferc.gov/market-assessments/guide/energy-primer.pdf]. In contrast to electricity and natural gas, the "Commission's jurisdiction over the oil sector is limited to setting pipeline transportation rates and ensuring open access in the pipeline system." *Id.*

15. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-332, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT CYBERSECURITY RISKS FACING THE ELECTRIC GRID 5 (2019) [hereinafter GAO-19-332], https://www.gao.gov/assets/710/701079.pdf, for a more detailed explanation of each function of the electricity sector. For a visualization of how generation, transmission, and distribution work together, see *id.* at 6.

16. *The Bulk-Power System*, WECC, https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/The-Bulk-Power-System.aspx (last visited Aug. 11, 2020); *see also* GAO-19-332, *supra* note 15, at 13 (defining the bulk power system as the "(1) facilities and control systems necessary for operating the electric transmission network and (2) the output from certain generation facilities needed for reliability").

17. *See* GAO-19-332, *supra* note 15, at 6. The nation's electric grid is comprised of the Eastern Interconnection, Western Interconnection, and Electric Reliability Council of Texas Interconnection. *Id.*

18. *See* EISEN ET AL., *supra* note 12, at 73–74 (explaining the unique nature of electricity and the grid's need for continuous balance).

19. *See* Oneok, Inc. v. Learjet, Inc., 135 S. Ct. 1591, 1595–96 (2015) (describing the traditional segmentation of the natural gas industry).

20. NAT. GAS COUNCIL, NATURAL GAS SYSTEMS: RELIABLE & RESILIENT 20–21 (2017), https://www.ngsa.org/download/analysis_studies/NGC-Reliable-Resilient-Nat-Gas-WHITE-PAPER-Final.pdf. Only interstate transportation and storage of natural gas are governed by the FERC's price regulation. *Id.* at 21.

Transmission pipelines carry natural gas across the country to distribution systems or large consumers (e.g., power plants, which are electric generators).[21] Specifically, interstate pipeline transmission is the key to the relationship between natural gas and electricity, and is the focus of this analysis.

B. The Interdependent Relationship Between Electricity and Natural Gas, and the Importance of Cybersecurity

Electric generation—the creation of electricity—is powered by a diverse portfolio of energy resources.[22] Natural gas is the biggest single resource powering the electric grid today, accounting for over 35% of electric generation in the United States.[23] The shale boom in the United States made the nation's electric grid and economy increasingly reliant on natural gas.[24] Since 2015, in attempt to meet market demand, natural gas companies have built additional pipelines and expanded delivery capabilities.[25] Typically, natural-gas-fired electric generators are directly connected to a natural gas pipeline, which supplies the generator with natural gas.[26] Thus, an attack that disrupts natural gas service or its transmission could have devastating effects on electric generation and the grid.[27] In this ever-connected relationship, the

---

21. *See Pipeline Glossary: Transmission Line*, U.S. DEP'T OF TRANSP., https://primis.phmsa.dot.gov/comm/glossary/index.htm?nocache=5064#TransmissionLine (last visited Aug. 11, 2020) (defining "transmission line" as "a pipeline used to transport natural gas from a gathering, processing or storage facility to a processing or storage facility, large volume customer, or distribution system").

22. *See supra* Part I.A (explaining the variety of energy resources that power the energy industry in the United States).

23. *See* GAO-19-332, *supra* note 15, at 34 n.61 (reporting natural gas as the leading electric generation resource).

24. *See* ENERGY PLAN, *supra* note 14, at 21. Additionally, the production and transmission of natural gas also relies on electricity, further deepening the connection between the two sectors. *Id.*

25. *See id.* (explaining that the demand for natural gas is so great that recent pipeline system expansions cannot meet demand); *see also* Joseph R. Dancy & Victoria A. Dancy, *Terrorism and Oil and Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks*, 2 OIL & GAS, NAT. RES. & ENERGY J. 579, 582 (2017) (discussing the increasing importance of pipeline cybersecurity following the increase of natural gas production in the United States).

26. *See* NAT. GAS COUNCIL, *supra* note 20, at 19–20 (discussing the purchasing practices of electric generators, which typically do not purchase their natural gas from the local natural gas distribution company).

27. *See, e.g.*, Clifford Krauss, *Cyberattack Shows Vulnerability of Gas Pipeline Network*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html ("[H]ackers could potentially jumble gas shipments[] and even

whole is only as strong as the weakest link. Hence, despite measures taken by the electricity sector to minimize cyber threats,[28] the grid remains exposed through the vulnerabilities of natural gas pipelines.[29]

Cyber threats are a legitimate risk to the nation's energy industry and could catastrophically disrupt the nation's economy and security, as well as the public's general welfare.[30] The energy sector accounted for 35% of the 796 cyber incidents reported by all critical infrastructure sectors; more incidents than any other sector.[31] In recent years, cyber threats have compromised both the electricity and natural gas pipeline sectors; yet, the regulatory response in each space of the industry has been alarmingly different.[32] The situation described at the beginning of this Comment is not a far-fetched, fantastical story. A February 2020 cyberattack on a natural gas compression facility shut down the facility for two days.[33] Although the attackers only struck one facility, the impact was sweeping.[34] Due to the interconnected nature of natural gas transportation, geographically distinct

---

cause electricity production outages."). A 2019 simulated cyberattack on the New York City area utility, serving 3.5 million people, highlighted the growing interdependence of gas and electricity, and the devastating impacts an outage could have on Wall Street and financial services. Robert Walton, *NERC's Simulated Grid Attack Leaves Thousands of New York Customers in Hypothetical Darkness*, UTIL. DIVE (Nov. 15, 2019), https://www.utilitydive.com/news/nercs-simulated-grid-attack-leaves-thousands-of-new-york-customers-in-hypo/567359/.

28. *See infra* Part III (discussing the mandatory cybersecurity standards in the bulk power system).

29. *See* Weber, *supra* note 6.

30. *Cybersecurity for Critical Energy Infrastructure*, U.S. DEP'T OF ENERGY, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure (last visited Aug. 11, 2020) (highlighting the nation's dependence on reliable energy to achieve national economic prosperity, security, and wellbeing).

31. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-48, CRITICAL INFRASTRUCTURE PROTECTION: ACTION NEEDED TO ADDRESS SIGNIFICANT WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT 12 (2018) [hereinafter GAO-19-48].

32. *See infra* A Brief Overview of the Current State of Cybersecurity Standards Part III (explaining the disparity in current cybersecurity standards for electricity and natural gas pipelines).

33. Kate O'Flaherty, *U.S. Government Issues Powerful Cyberattack Warning as Gas Pipeline Forced into Two Day Shut Down*, FORBES (Feb. 19, 2020, 8:44 AM), https://www.forbes.com/sites/kateoflahertyuk/2020/02/19/us-government-issues-powerful-cyberattack-warning-as-gas-pipeline-forced-into-two-day-shut-down/#5e7cac025a95. When a facility employee clicked a malicious email link, the attackers infiltrated the facility's IT network and then accessed its operational technology network. *Id.* This single facility experienced "loss of availability" on "human machine interfaces [], data historians, and polling servers." *Id.*

34. *Id.*

compression facilities also shut down, which resulted in a total "operational shutdown of the entire pipeline for two days."[35]

Since at least 1990, national researchers and technical experts have reported that a small number of well-informed cyberattackers could shut down the nation's entire electric grid for days or even months.[36] In 2017, Russian Advanced Persistent Threat Actors compromised U.S. energy companies and obtained enough control of the electric grid to induce power blackouts across the country.[37] In 2018, a large cyberattack on multiple pipeline companies across the United States shut down pipeline communication systems.[38] While that attack did not actually disrupt gas service, it demonstrated the extreme vulnerabilities of the nation's pipeline infrastructure.[39]

II. THE PATCHWORK OF FEDERAL AGENCIES AND OFFICES WITH AUTHORITY OVER THE ENERGY INDUSTRY

A. U.S. Department of Energy

The Department of Energy Organization Act of 1977 established the DOE.[40] The DOE is a cabinet-level agency concerned with the nation's nuclear activity and energy programs.[41] The federal government designated the DOE as the lead sector-specific agency for the cybersecurity of the energy sector, which includes protecting the nation's critical energy infrastructure from cyber threats.[42]

In 2013, Executive Order 13,636 prompted the DOE to collaborate with industry partners to develop the Energy Sector Cybersecurity Framework

35. *Id.*

36. *See* COMM. ON ENHANCING THE ROBUSTNESS & RESILIENCE OF FUTURE ELEC. TRANSMISSION & DISTRIB. IN THE U.S. TO TERRORIST ATTACK, NAT'L RSCH. COUNCIL, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM 9 (2012), https://www.nap.edu/read/12050/chapter/1 (citing a 1990 study reporting that some terrorist groups are capable of taking down U.S generation or transmission facilities).

37. Francesca Gargano, *Afraid of the Dark: Cyber Threats to the Energy Sector (Part One)*, LOOKINGGLASS CYBER: THREAT INTEL. BLOG (July 18, 2019), https://www.lookingglasscyber.com/blog/afraid-of-the-dark-cyber-threats-to-the-energy-sector-part-one/. While this incident did not cause any blackouts, a similar attack caused blackouts across Ukraine's electric grid in 2015 and 2016. *Id.*

38. Krauss, *supra* note 27.

39. *Id.*

40. Pub. L. No. 95-91, 91 Stat. 565 (codified as amended at 42 U.S.C. § 7101).

41. *A Brief History of the Department of Energy*, U.S. DEP'T OF ENERGY, https://www.energy.gov/lm/doe-history/brief-history-department-energy (last visited Aug. 11, 2020).

42. ENERGY PLAN, *supra* note 14, at 8–9.

Implementation Guidance.[43] The Energy Sector Cybersecurity Framework Implementation Guidance, using both the National Institute of Standards and Technology (NIST) Cybersecurity Framework and then-existing industry standards, tools, and processes,[44] helped "characterize, enhance, and communicate" the energy industry's approach to cybersecurity.[45] Furthermore, the DOE developed two Cybersecurity Capability Maturity Model (C2M2) programs—one for the electricity sector and one for the oil and natural gas sectors—to help "evaluate, prioritize, and improve cybersecurity released a multi-year plan for energy sector cybersecurity, which attempts to strengthen delivery systems and develop cutting-edge cyber solutions.[46]

In 2018, as a response to the increasing magnitude and sophistication of threats to the nation's energy infrastructure,[47] the DOE established the Office of Cybersecurity, Energy Security, and Emergency Response.[48] This Office is responsible for ensuring the electric grid and the natural gas pipeline systems are resistant to cyber threats.[49] Beyond preventing cybersecurity attacks, this Office also focuses on enabling coordinated preparation and response to natural and man-made threats to the nation's energy.[50]

Within the Office of Cybersecurity, Energy Security, and Emergency Response, the Cybersecurity for Energy Delivery Systems Division leads

---

43. *Id.* at 14.

44. The National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework to provide voluntary guidance for the nation's critical infrastructures to manage and reduce cybersecurity threats. *New to Framework: Background*, NIST (Feb. 5, 2018), https://www.nist.gov/cyberframework/new-framework.

45. ENERGY PLAN, *supra* note 14, at 14.

46. *See* OFF. OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, MULTI-YEAR PLAN FOR ENERGY SECTOR CYBERSECURITY 5–6 (2018) (listing three goals: (1) strengthen cybersecurity preparedness; (2) coordinate cyber incident response and recovery; and (3) accelerate game-changing research and development of resilient energy delivery systems).

47. Brandi Vincent, *The Budding Office of Cybersecurity, Energy Security and Emergency Response Aims to Deflect Cyber, Manmade and Natural Security Hazards*, NEXTGOV (Mar. 21, 2019), https://www.nextgov.com/cybersecurity/2019/03/how-energy-department-prioritizing-secure-infrastructure/155734/ (providing reasoning for the Office's creation).

48. *See* Press Release, U.S. Dep't of Energy, Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response (Feb. 14, 2018), https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency (announcing the Office's creation in February 2018).

49. *Cybersecurity for Critical Energy Infrastructure*, *supra* note 30 (highlighting the nation's dependence on reliable energy to achieve national economic prosperity, security, and wellbeing); *see also supra* Part I.B (discussing resiliency in the energy sector).

50. Press Release, U.S. Dep't of Energy, *supra* note 48. Secretary of Energy Rick Perry established this Office with funding included in President Trump's FY 2019 budget request. *Id.*

research and development to improve the security of the nation's critical energy infrastructure from cyber threats.[51] This Division has three main areas of activity: "strengthening energy sector cybersecurity preparedness[,] coordinating cyber incident response and recovery[, and] accelerating research, development and demonstration [] of game-changing and resilient energy delivery systems."[52] While this Office can create voluntary tools, programs, and best practices for the energy industry, it does not have any regulatory authority to mandate implementation or enforce compliance.[53]

B. The Federal Energy Regulatory Commission

The FERC is an independent agency housed within the DOE.[54] As an independent agency, the Commission is insulated from overly broad oversight or undue political influence from the President, Congress, or a private party.[55] The Commission derives its regulatory power over the

51. *Cybersecurity for Critical Energy Infrastructure*, *supra* note 30.

52. *Id.*

53. *See Energy Sector Cybersecurity Preparedness*, U.S. DEP'T OF ENERGY, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity (last visited Aug. 11, 2020); *see also* Brigham A. McCown, *Can Congress Bolster Energy Cyber Protections?*, FORBES (May 22, 2019, 7:45 AM), https://www.forbes.com/sites/brighammccown/2019/05/22/cybersecurity/#6ba934fa16ab (applauding the Department of Energy (DOE) for "doing its part" through the Office of Cybersecurity, Energy Security, and Emergency Response's research and development projects).

54. *See* 42 U.S.C. § 7171(a) (creating a statutorily-independent regulatory agency). In 1920, Congress established the Federal Power Commission, the Commission's predecessor, which became an independent agency in 1935. *See* Pub. L. No. 66-280, ch. 285, 41 Stat. 1063 (1920) (codified as amended 16 U.S.C. § 792) (creating the Federal Power Commission in 1920); Pub. L. No. 74-333, 49 Stat. 803 (establishing the Federal Power Commission as an independent agency). The Department of Energy Organization Act of 1977 created and divided federal energy authority between the DOE and the FERC. Sharon B. Jacobs, *The Statutory Separation of Powers*, 129 YALE L.J. 378, 383 (2019). Congress first created the Commission in 1977, and it inherited most of the Federal Power Commission's responsibilities; however, Congress originally delegated some responsibilities to the DOE. *See* Department of Energy Organization Act, Pub. L. No. 95-91, §§ 204, 402(a), 91 Stat. 565, 571, 583–84 (1977) (codified as amended 42 U.S.C. §§ 7134, 7172(a)); Greenfield, *supra* note 10, at 3. The DOE's responsibilities were subsequently delegated to the Commission through Department of Energy Delegation Order No. 00-004-00A. *Id.*

55. *See* Greenfield, *supra* note 10, at 3 (explaining that the FERC is an independent entity because no more than three of the five Commissioners can come from one political party, a court reviews the FERC's decisions, and private parties in court proceedings are prohibited from ex parte discussions with the Commissioners or staff).

electricity and natural gas sectors from two main statutes: the Federal Power Act (FPA)[56] and the NGA.[57]

The FPA gives the Commission exclusive authority over interstate transportation and wholesale of electricity.[58] The Energy Policy Act of 2005 further expanded the Commission's authority to oversee the reliability of the bulk power system, create an Electric Reliability Organization, and approve mandatory cybersecurity reliability standards and associated penalties.[59] The Commission designated the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization.[60]

Similarly, the NGA gives the Commission its authority over natural gas.[61] Today, the Commission regulates pipeline transmission rates and issues certificates of public convenience and necessity.[62] The Commission has jurisdiction over three separate areas within the natural gas sector: (1) the transportation of natural gas in interstate commerce; (2) the sale of natural gas in interstate commerce for resale; and (3) natural gas companies engaged in such transportation or sale.[63] While the Commission does not have unlimited authority in a single one of these areas, courts have held that activity touching all three areas triggers Commission regulation.[64]

---

56. Federal Power Act (FPA), 16 U.S.C. § 824.

57. Natural Gas Act (NGA), 15 U.S.C. § 717.

58. FERC v. Elec. Power Supply Ass'n, 136 S. Ct. 760, 766 (2016); Hughes v. Talen Energy Mktg., LLC, 136 S. Ct. 1288, 1291 (2016).

59. 16 U.S.C. § 824o (listing what is commonly known as Section 215 of the FPA).

60. *See infra* Part II.C.

61. 15 U.S.C. § 717 (giving the Federal Power Commission this responsibility, which was later conferred to the Commission). Section 717(b) provides the Commission with natural gas jurisdiction over "the transportation of natural gas in interstate commerce," wholesale of natural gas, "to natural-gas companies engaged in such transportation or sale," and international import and export of natural gas and persons involved in such trade. § 717(b). FERC jurisdiction does not extend to intrastate transportation, retail sales, distribution, production, or gathering facilities of natural gas. *See id.*

62. Pursuant to § 7 of the NGA, a certificate of public convenience and necessity is required before any natural gas company constructs an interstate pipeline and engages in the sale of natural gas. § 717(c).

63. Order Denying Rehearing, 155 FERC ¶ 61,184, at 4 (May 19, 2016) (citing 15 U.S.C. § 717(1)(b)) (on file with the *Administrative Law Review*).

64. City of Clarksville v. FERC, 888 F.3d 477, 480 (D.C. Cir. 2018); *see also* Pub. Serv. Co. of N.C. v. FERC, 587 F.2d 716, 720 (5th Cir. 1979) (emphasizing "the convergence of three factors—(1) interstate transmission by a natural gas company, (2) Commission certification, and (3) the state's acquiescence in (1) and (2)" that subjected the state to FERC regulation). In *City of Clarksville*, the court held the Commission did not have authority to regulate the City's natural gas sale to Guthrie—a Kentucky municipality. 888 F.2d at 485–86. While the City acquiesced to the FERC's jurisdiction when it applied for a Section 7

C. The North American Electric Reliability Corporation

Following the Energy Policy Act of 2005, the Commission designated and approved the NERC as the national electric reliability organization.[65] The NERC is a not-for-profit international corporation dedicated to reducing risks to the reliability and security of the grid.[66] As the nation's sole electric reliability organization, NERC has the power to impose penalties on owners and operators of the bulk power system for violating its established reliability standards. However, the Commission oversees the NERC's activities and approves its proposed standards and sanctions.[67]

D. Transportation Security Administration

The TSA is housed within the U.S. Department of Homeland Security (DHS).[68] Although best known for its airport security efforts,[69] the TSA is

service area determination to service interstate customers via its distribution facilities and interstate pipelines, it only acquiesced to jurisdiction for those distribution channels. *Id.* at 480, 486. It did not acquiesce to the FERC's jurisdiction regarding the sale to Guthrie because it was not using its interstate pipelines or facilities during this sale. *Id.* at 486.

65. 16 U.S.C. § 824o(b), (d)-(e); *see* Alcoa Inc. v. FERC, 564 F.3d 1342, 1344–45 (D.C. Cir. 2009) (explaining the process NERC went through to become the national electric reliability organization). Before becoming the single entity approved by the Commission to oversee electric reliability, NERC was a voluntary reliability organization that issued nonbinding guidelines and standards for the bulk power system. *Id.*

66. *See About NERC*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/AboutNERC/Pages/default.aspx (last visited Aug. 11, 2020) (describing NERC's mission, authority, and jurisdiction).

67. *See* 16 U.S.C. § 824o(b)(1), (c)(2)(C), (d)(1)(2) (stating that the Commission may approve certain reliability standards that The Electric Reliability Organization proposes).

68. *See* Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101, 115 Stat. 597 (2001) (codified as amended 49 U.S.C. § 114(d)) (establishing the TSA on November 19, 2001); *see also* 6 U.S.C. § 203(2) (transferring the TSA from the Department of Transportation (DOT) to the Department of Homeland Security (DHS)).

69. *See* Jay Wagner, *TSA Year in Review: A Record Setting 2018*, TRANSP. SEC. ADMIN.: BLOG (Feb. 7, 2019), https://www.tsa.gov/blog/2019/02/07/tsa-year-review-record-setting-2018 (recording a total of 813.8 million people passing through TSA airport security screenings in 2018). In addition to over 800 million yearly aviation passengers and nearly three million miles of pipelines, the TSA oversees 138,000 miles of railroad tracks and four million miles of highway. Neil Chatterjee & Richard Glick, *Cybersecurity Threats to U.S. Gas Pipelines Call for Stricter Oversight*, AXIOS, https://www.axios.com/cybersecurity-threats-to-us-gas-pipelines-call-for-stricter-oversight-09fac6e5-da94-491e-9523-d08ef15237f4.html (last updated June 11, 2018).

the federal entity responsible for security in all modes of transportation, including the nation's interstate pipeline system.[70]

The TSA first began its pipeline security efforts in 2002 by leveraging the Department of Transportation (DOT) Office of Pipeline Security's Information Circular.[71] The TSA also adopted and issued other planning guidance for pipeline security from the DOT.[72] After almost a decade of pipeline security responsibility, the TSA created the 2010 Pipeline Security Guidelines and updated them the following year.[73] Prompted by growing physical and cybersecurity threats, the TSA updated and reissued its guidelines in 2018.[74]

Despite creating and distributing its own pipeline security guidelines, significant weaknesses exist in the TSA's approach to pipeline cybersecurity.[75] Perhaps the most notable vulnerability is the limited number of TSA personnel assigned to interstate pipelines—a critically important national security commodity.[76] In recent years, the TSA has employed only between one and fourteen full-time TSA agents to manage the physical security and cybersecurity of the three million miles of U.S. pipelines.[77]

---

70. *See* 49 U.S.C. § 114(d)(2), (f)(7) (giving TSA 's head the "security responsibilities over other modes of transportation that are exercised by the [DOT]" and the power to "enforce security-related regulations and requirements"). Pipelines are a mode of transportation within the TSA's purview. *See* § 114(u)(1)(E).

71. *See* TRANSP. SEC. ADMIN., U.S. DEP'T OF HOMELAND SEC., PIPELINE SECURITY GUIDELINES 1 (2018) [2018 PIPELINE GUIDELINES], https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

72. *Id.*

73. *Id.* No obvious explanation seems to exist as to why the TSA published its updated guidelines so quickly. Both documents contain the same "purpose" statement. *Compare* TRANSP. SEC. ADMIN., U.S. DEP'T OF HOMELAND SEC., PIPELINE SECURITY GUIDELINES 1 (2010) (on file with the *Administrative Law Review*), *with* TRANSP. SEC. ADMIN., U.S. DEP'T OF HOMELAND SEC., PIPELINE SECURITY GUIDELINES 1 (2011), https://www.hsdl.org/?view&did=750295.

74. *See generally* 2018 PIPELINE GUIDELINES, *supra* note 71 (updating the TSA's guidelines and issuing the TSA's latest guidance).

75. *See* GAO-19-48, *supra* note 31, at 62–63 (auditing the TSA's pipeline security efforts and recommending ten specific actions to minimize pipeline cyber vulnerabilities).

76. *See id.* at 38–39 (demonstrating that the total number of TSA personnel dedicated to pipeline security ranged from fourteen to one from 2010 through 2018).

77. *See id.* As of 2017, the number of full-time TSA agents responsible for the nation's nearly three million miles of pipeline totaled a dismal six employees. *See* Chatterjee & Glick, *supra* note 69 (suggesting the DOE is better suited to oversee pipeline cybersecurity standards).

Additionally, the TSA does not make any of its cybersecurity recommendations or best practices mandatory for pipeline owners.[78]

E. Cybersecurity and Infrastructure Security Agency

Another agency within the DHS, the Cybersecurity and Infrastructure Security Agency (CISA), develops pipeline security guidelines.[79] The CISA advances partnerships across the public and private sectors to provide technical assessments and resources for critical infrastructure stakeholders.[80] Recently, the CISA collaborated with the TSA to start the Pipeline Cybersecurity Initiative Fact Sheet.[81] This initiative intends to bring together the pipeline sector-specific expertise of the TSA and the technical capabilities of the CISA to better protect pipelines.[82] Published in March 2019, the Initiative Fact Sheet proposes three different types of voluntary assessments for pipelines to mitigate cyber vulnerabilities.[83] Again, these pipeline cyber assessments are not required of pipeline owners or operators; yet, the assessments are expected to develop a long-term cybersecurity strategy to combat emerging threats to pipelines.[84]

---

78. *See* 2018 PIPELINE GUIDELINES, *supra* note 71. No clear answer exists as to why the TSA does not implement mandatory standards on natural gas pipelines, but many suggest the agency lacks the staff and resources to develop these standards. *See* John Siciliano, *Fight Brewing over Pipeline Security*, WASH. EXAM'R (Feb. 15, 2019, 12:00 AM), https://www.washingtonexaminer.com/policy/energy/fight-brewing-over-pipeline-security. FERC Commissioner Glick suggests that the Commission could exercise more oversight over interstate pipelines than the TSA's demonstrated abilities, but he recognizes the Commission's lack of intrastate pipeline jurisdiction could limit the FERC's pipeline cybersecurity regulations. Troutman Pepper Pipeline Practice, *Pipeline Security and Cybersecurity: Are Guidelines Enough to Protect Critical Infrastructure?*, PIPELAWS (June 4, 2018), https://www.pipelaws.com/2018/06/pipeline-security-cybersecurity-guidelines-enough-protect-critical-infrastructure.

79. *See About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about-cisa (last visited Aug. 11, 2020).

80. *Id.*

81. *Pipeline Cybersecurity Initiative*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Mar. 5, 2019), https://www.dhs.gov/cisa/pipeline-cybersecurity-initiative.

82. *Pipeline Cybersecurity Initiative Fact Sheet*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Mar. 5, 2019), https://www.cisa.gov/sites/default/files/publications/19_0305_cisa_pipeline-cybersecurity-initiative-fact-sheet.pdf.

83. The TSA and the Cybersecurity and Infrastructure Security Agency (CISA) work with the industry partner to execute Tier-I assessments (multi-day evaluations) and Tier-II assessments (single-day evaluations). *Id.* Tier-III self-assessments are completed exclusively by the pipeline owners on their own volition. *Id.*

84. *Pipeline Cybersecurity Initiative*, *supra* note 81.

F. Department of Transportation

All interstate pipelines are subject to safety standards established by the Pipeline and Hazardous Material Safety Administration within the DOT.[85] In 2006, the Pipeline and Hazardous Material Safety Administration and the TSA agreed to delineate clear roles within their overlapping pipeline security authority.[86] The agencies arranged that the TSA is the lead entity for transportation security, including pipeline security, and that the Pipeline and Hazardous Material Safety Administration is responsible for administering a national program of safety in natural gas pipeline transportation, including identifying pipeline safety concerns and developing uniform standards.[87]

III. A BRIEF OVERVIEW OF THE CURRENT STATE OF CYBERSECURITY STANDARDS

The interstate electricity sector, known as the bulk power system, must comply with the NERC's Critical Infrastructure Protection Standards (NERC CIP Standards).[88] The NERC developed the NERC CIP Standards in 2003 "to establish a baseline set of security measures across the sector,"[89] and made them a mandatory requirement for the bulk power system in 2008.[90] Demonstrating its commitment to cybersecurity,[91] the FERC recently approved additional mandatory cybersecurity reporting

85. GAO-19-48, *supra* note 31, at 21–22.

86. *Id.* This is another example of overlapping agency claims over pipeline security efforts and a possible solution when agency roles are unclear or ill-defined. *Id.*

87. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-426, CRITICAL INFRASTRUCTURE PROTECTION: KEY PIPELINE SECURITY DOCUMENTS NEEDED TO REFLECT CURRENT OPERATING ENVIRONMENT 2 (2019), https://www.gao.gov/assets/700/699511.pdf.

88. *See NERC-CIP Requires Vulnerability Assessment*, BEYOND SEC., https://beyondsecurity.com/vulnerability-assessment-requirements-nerc-cip.html?cn-reloaded=1 (last visited Aug. 11, 2020). NERC's Critical Infrastructure Protection Standards (NERC CIP Standards) are the threshold requirement for cybersecurity compliance as a bulk power system player. *Id.*

89. Josh Perri, *The NERC CIP Standards: An Overview to Foster Compliance*, IS PARTNERS, https://www.ispartnersllc.com/blog/nerc-cip-standards-overview/ (last updated Sept. 27, 2018).

90. Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 324 (2013).

91. *See, e.g.*, Cyber Security Incident Reporting Reliability Standards, 164 FERC ¶ 61,033, at 7 (2018), https://www.ferc.gov/sites/default/files/2020-04/E-1_4.pdf (ordering NERC to promulgate a new rule addressing utilities underreporting of cyber incidents, which include both executed and attempted cyberattacks).

standards for the bulk power systems.[92] The NERC CIP Standards include guidelines for cyber incidents reporting, attempted incidents reporting, response planning, identification of critical cyber assets, personnel and training, and physical and digital security systems and management.[93] These standards are mandatory, and failure to comply comes at a hefty cost for electric organizations.[94] In February of 2019, NERC issued a $10 million fine to an electric utility for repeatedly violating the NERC CIP Standards.[95]

Despite setting forth these standards for the electricity sector, regulators do not require natural gas pipelines to meet any mandatory cybersecurity standards.[96] While many agencies are involved in pipeline security, the TSA is the ultimate federal agency responsible for cybersecurity of the nation's pipeline network.[97] While the TSA has continuously updated its pipeline cybersecurity guidelines, it has refused to impose any mandatory regulations or noncompliance penalties.[98] Although the TSA's voluntary Pipeline Security Guidelines incorporate most of the best practices from

92. N. Am. Elec. Reliability Corp., 167 FERC ¶ 61,230, at 1 (2019), https://www.ferc.gov/sites/default/files/2020-05/E-2_46.pdf (approving NERC's proposed additional CIP Standard); *see generally* Press Release, FERC, FERC Strengthens Cyber Security Standards for Bulk Electric System (June 20, 2019), https://www.ferc.gov/news-events/news/ferc-strengthens-cyber-security-standards-bulk-electric-system (highlighting certain aspects of approved FERC measures).

93. Aaron Lang, *FERC and NERC Talk Grid Resilience and Cybersecurity*, JD SUPRA (Apr. 3, 2019), https://www.jdsupra.com/legalnews/ferc-and-nerc-talk-grid-resilience-and-22836/. For the specific measures required by each standard, see Justin Peacock, *How to Know You Meet NERC CIP Cybersecurity Requirements*, SEC. BOULEVARD (Feb. 18, 2020), https://securityboulevard.com/2020/02/how-to-know-you-meet-nerc-cip-cybersecurity-requirements/.

94. NERC can impose $1 million per violation, per day, for failure to conform with the NERC CIP Standards. Siciliano, *supra* note 78.

95. Iulia Gheorghiu, *Duke Fined $10M for Cybersecurity Lapses Since 2015*, UTIL. DIVE (Feb. 4, 2019), https://www.utilitydive.com/news/duke-fined-10m-for-cybersecurity-lapses-since-2015/547528/.

96. *See* 2018 PIPELINE GUIDELINES, *supra* note 71 (publishing the TSA's only cybersecurity measures for pipelines, and stating "[t]his document is guidance and does not impose requirements on any person or company").

97. *See, e.g.*, PARFOMAK, *supra* note 5 ("The [TSA] is authorized by federal statute to promulgate pipeline physical security and cybersecurity regulations . . . .").

98. *See* 2018 PIPELINE GUIDELINES, *supra* note 71 ("This document is guidance and does not impose requirements on any person or company. The term '*should*' means that TSA recommends the actions described. Nothing in this document shall supersede Federal statutory or regulatory requirements.") (emphasis added); *see also supra* text accompanying note 78.

the NIST Framework for Improving Critical Infrastructure Cybersecurity, the TSA did not incorporate all principles, and it has no documented process for reviewing and revising its voluntary guidelines in the future.[99]

IV. RECOMMENDATIONS

As an independent agency specializing in energy regulation, including electricity and natural gas pipelines,[100] the Commission should be the federal agency with ultimate regulatory authority over natural gas pipeline cybersecurity standards. To do so, this Comment recommends two options. First, Plan A: the Commission should reinterpret the scope of its authority under the NGA. Alternatively, Plan B: Congress should pass an Act expressly vesting the Commission with interstate natural gas pipeline cybersecurity jurisdiction. Both plans then recommend the Commission designate a natural gas reliability organization to develop and enforce mandatory cybersecurity regulations.

A. Task the FERC with Interstate Natural Gas Pipeline Cybersecurity Standards

The disparity in cybersecurity standards between the bulk power system and natural gas pipelines is alarming.[101] The different characteristics of electricity and natural gas create a natural division in the energy industry, which leads to disparate treatment.[102] While this bifurcated approach worked in the past, it is no longer a plausible solution to cyber threats in an increasingly connected and interdependent industry.[103] Today, where the

99. Ionut Arghire, *TSA Lacks Cybersecurity Expertise to Manage Pipeline Security Program: Report*, SEC. WK. (May 2, 2019), https://www.securityweek.com/tsa-lacks-cybersecurity-expertise-manage-pipeline-security-program-report.

100. *See supra* Part II.B.

101. *Compare Pipeline Cybersecurity Initiative Fact Sheet*, *supra* note 82 (describing the three different types of voluntary assessments that the TSA and the CISA will use to better protect pipelines), *with* N. Am. Elec. Reliability Corp., 167 FERC ¶ 61,230, at 1 (2019), https://www.ferc.gov/whats-new/comm-meet/2019/062019/E-2.pdf (expanding the reporting requirements for the bulk electric system, which now include both attempted cyberattacks and cyberattacks that compromised or disrupted the grid's operation).

102. For example, while natural gas can be directly consumed to provide heat, power equipment, and other tasks, electric power is a result of using energy resources, such as natural gas, in the generation stage. *Natural Gas Explained: Use of Natural Gas*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/energyexplained/natural-gas/use-of-natural-gas.php (last updated July 22, 2020).

103. *See* ENERGY PLAN, *supra* note 14, at 21.

Internet of Things[104] rapidly connects systems and networks, a unified front is the strongest defense to Internet threats.[105]

The FERC, not the TSA, should—in addition to its oversight over the electricity sector—be the agency with ultimate oversight responsibility and authority over interstate natural gas pipeline cybersecurity standards. While the Commission's enabling statutes—the FPA and the NGA—are discrete, the Commission should have parallel authority over natural gas pipeline cybersecurity to protect our national security interests. Unlike the TSA, the Commission has the energy sector-specific knowledge that will lead to effective and meaningful cybersecurity standards for pipelines.[106]

The Commission's status as an independent agency,[107] in addition to its industry expertise and consistency, can encourage consistent development of long-term cybersecurity goals in ways the TSA cannot.[108] The FERC's status as an independent agency allows for bipartisan decisionmaking that best serves a national interest as significant as security of the nation's energy.[109] Furthermore, the Commission's status as an independent agency enhances the longevity of the agency's initiatives and institutional knowledge.[110]

---

104. The Internet of Things refers to the billions of physical devices that, through their connection to the Internet, collect and share data in real time, often without any human involvement. Steve Ranger, *What is the IoT? Everything You Need to Know About the Internet of Things Right Now*, ZDNET (Feb. 3, 2020, 2:45 PM), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

105. *See 2019 Cybersecurity Awareness Symposium*, FED. BUS. COUNCIL, INC., https://www.fbcinc.com/e/DoCITCyber/ (last visited Aug. 11, 2020) (dedicating a conference theme of "A Unified Front," and highlighting policies and standards as a main component to interagency cybersecurity efforts); Troutman Pepper Pipeline Practice, *supra* note 78 ("Commissioner Glick commented that '[i]f you just have one weak link—one entity that doesn't follow [the oil and gas pipeline industry's] voluntary standards—it can cause significant damage.'").

106. The Commission and its predecessor, the Federal Power Commission, have one-hundred years of combined experience in the energy sector. *See* Greenfield, *supra* note 10, at 3 (dating the Federal Power Commission's 1920 establishment).

107. 42 U.S.C. § 7171(a).

108. *See* MICHAEL LEWIS, THE FIFTH RISK 45 (2018) (describing the turnover in executive agencies during administration changes).

109. Independent agencies run by multi-member boards or commissions bring together industry expertise and diverse views that can "tackle legally difficult, technically complex, and often politically sensitive issues." Marshall J. Berger & Gary J. Edles, *Established by Practice: The Theory and Operation of Independent Federal Agencies*, 52 ADMIN. L. REV. 1111, 1112 (2000). The FERC, led by a bipartisan five-member commission, is one such agency. 42 U.S.C. § 7171(b)(1). Commissioners are appointed by the President and approved by the Senate, and not more than three Commissioners can be members of the same political party at a given time. *Id.*

110. *See* LEWIS, *supra* note 108 (stating that ushering in a new presidential administration means a change in agency leadership with no guarantee of consistency or knowledge). For

Conversely, the TSA is an executive-governed agency.[111] The distinction between an independent agency and an executive-governed agency may seem slight, but it could mean the difference between comprehensive and inadequate national security.[112] While the TSA is mute on whether it is inclined to relinquish or bolster its authority in the pipeline-cybersecurity space, lawmakers are keen on enhancing the DHS's, and the TSA's, power to take on evolving threats to national security.[113]

1. Plan A

To vest the Commission with regulatory authority over the natural gas pipeline cybersecurity standards, the Commission should reinterpret its authority under the NGA. First, the Commission should look to its

example, when the Trump Administration was preparing to take office in 2017, 138 political appointees in the DOE were required to resign, including the employee responsible for the nation's nuclear-weapon program. *Id.* Only the "keeper of the nation's nuclear secrets" was asked to return—the day before Trump's inauguration—to work at the DOE. *Id.* The rest of the institutional knowledge walked out the door with the 137 other employees. *Id.*

111. *See The Executive Branch*, THE WHITE HOUSE: PRESIDENT BARACK OBAMA, https://obamawhitehouse.archives.gov/1600/executive-branch (last visited Aug. 11, 2020) (creating the DHS, an executive-governed agency that houses the TSA, consolidated twenty-two other Executive Branch agencies).

112. While the President appoints and the Senate confirms, both independent and executive-governed agency heads, the major differentiating factor is that the President cannot remove an independent agency head for political reasons. Humphrey's Ex'r v. United States, 295 U.S. 602, 631–32 (1935) (ruling that the President's power to remove executive officers does not extend to agency commissioners who serve legislative and judicial functions). The President's ability to remove a commissioner is statutorily confined. Wiener v. United States, 357 U.S. 349, 356 (1958) (denying the President the power to remove an independent agency commissioner for political cause, unless statutorily permitted). Thus, independent agencies and their commissioners are theoretically insulated from pressure and punitive threats by a President. *See id.*

113. *See* Maggie Miller, *House Homeland Security Republicans to Introduce Slew of Cybersecurity Bills*, THE HILL (June 18, 2019, 5:30 AM), https://thehill.com/policy/cybersecurity/448971-house-homeland-security-republicans-to-introduce-slew-of-cybersecurity (detailing the bills that congressmen anticipate introducing that comprise the "American Security Agenda"). Interestingly, of the anticipated bills, the Pipeline Security Enhancement Act—which would give the TSA inspection authority over pipeline security—is not included in the many bills that lawmakers have introduced. *See American Security Agenda*, HOMELAND SEC. REPUBLICANS, https://republicans-homeland.house.gov/legislative-agenda/ (last visited Aug. 11, 2020). All TSA-related pending legislation contains no mention of pipeline cybersecurity. *See generally* H.R. 5828, 116th Cong. (2020); H.R. 4402, 116th Cong. (2019); Emerging Transportation Security Threats Act of 2019, H.R. 3318, 116th Cong. (2019).

jurisdictional authority under § 1(b) of the NGA.[114] Relying on the express language of the statute, the Commission should find it can impose reliability regulations on interstate pipelines and natural-gas companies engaged in interstate transmission.

The Commission should introduce a reliability organization and cybersecurity standards, just as it did for the electricity sector.[115] The FPA, giving the Commission federal regulatory authority over the electricity sector, and the NGA, vesting the Commission with regulatory authority over interstate natural gas pipelines, have been analogized and used interchangeably by the Supreme Court when determining the scope of the Commission's authority.[116] However, while the Commission approves cybersecurity standards over the electricity sector, it currently does not exercise any cybersecurity authority over the natural gas sector despite its historically parallel authority in the two sectors.

The Supreme Court routinely relies on cases discussing the FPA to determine the Commission's scope of authority in the natural gas sector.[117] Additionally, the NGA was modeled substantively after the FPA and courts have interpreted the two statutes similarly.[118] Likewise, the Commission should reinterpret its natural gas pipeline authority and then determine it has the regulatory authority to impose cybersecurity standards on natural gas pipelines.[119] The natural gas industry, represented by associations and other national organizations, and possibly other federal agencies, will likely

---

114. *See supra* text accompanying note 61.

115. *See* N. Am. Elec. Reliability Corp., 167 FERC ¶ 61,230, at 1 (2019), https://www.ferc.gov/whats-new/comm-meet/2019/062019/E-2.pdf.

116. *See* Hughes v. Talen Energy Mktg., LLC, 136 S. Ct. 1288, 1298 n.10 (2016) (explaining that although *Oneok, Inc. v. Learjet, Inc.*, 135 S. Ct. 1591 (2015), involved the NGA rather than the FPA, the relevant provisions of the two statutes are analogous, and citing *Oneok* in a case discussing the FPA is appropriate).

117. *Hughes*, 136 S. Ct. at 1298 n.10; *see also Oneok, Inc.*, 135 S. Ct. at 1601–02 (relying on the FPA to determine the Commission's scope of authority under the NGA).

118. City of Clarksville v. FERC, 888 F.3d 477, 484 (D.C. Cir. 2018); *see also* Tenn. Gas Pipeline Co. v. FERC, 860 F.2d 446, 454 (D.C. Cir. 1988) ("The Supreme Court has held that the NGA and the FPA are in all material respects substantially identical and constructions of one are authoritative for the other.").

119. This would not be the first time the FERC has expanded its jurisdiction under the NGA. In Order No. 670, the FERC interpreted § 4A of the NGA as broadening its authority over the previously limiting § 1(b) of the Act. *See* William F. Demarest, Jr., *"Traditional" NGA Jurisdictional Limits Constrain FERC's Market Manipulation Authority*, 31 ENERGY L.J. 471, 476–77 (2010) (explaining the FERC's expansive reading of its authority under the NGA).

challenge the Commission's reinterpretation of its authority in the courts.[120] Litigation may delay the Commission's ability to act on that authority and implement pipeline cyber standards. While the congressional intent behind enacting the NGA was to fill a regulatory gap,[121] rather than occupy the entire field, expanding the FERC's jurisdiction to include interstate natural gas pipeline cybersecurity standards only incrementally expands the scope of what it already regulates.[122]

To facilitate this interagency change in federal regulators, the Commission should sign a memorandum of understanding with the TSA to assign regulatory responsibility and streamline regulatory oversight.[123] Like the TSA's agreement with Pipeline & Hazardous Material Safety Administration, the Commission and the TSA should agree to draw a hard line in the sand.[124] In doing so, the TSA should relinquish its cybersecurity authority but retain its physical security authority.[125]

---

120. *See* Blake Sobczak, *Battle Lines Form over Pipeline Cyberthreat*, E&E NEWS (July 25, 2019), https://www.eenews.net/stories/1060784805 (suggesting likely industry challengers and the industry's preference for TSA-controlled, unprescribed standards). The Commission previously faced off in the courts after reinterpreting its natural gas jurisdiction. *See City of Clarksville*, 888 F.3d at 483 (rejecting both the Commission's reinterpretation of "person" in the NGA and its expanded jurisdiction over municipalities under 15 U.S.C. § 717(b)).

121. "The NGA was intended to fill the regulatory gap left by a series of Supreme Court decisions that interpreted the dormant Commerce Clause to preclude state regulation of interstate transportation and of wholesale gas sales." United Distrib. Cos. v. FERC, 88 F.3d 1105, 1122 (D.C. Cir. 1996).

122. *See supra* Part II.B (outlining the FERC's regulatory authority).

123. The Commission is no stranger to interagency memoranda of understanding. For example, in July 2018, the Commission announced it agreed with the Pipeline and Hazardous Materials Safety Administration of the DOT, which previously housed the TSA, to enter into a memorandum of understanding for reviewing and approving proposed liquefied natural gas facilities. Press Release, U.S. Dep't of Transp., PHMSA, FERC to Sign Memorandum of Understanding to Strengthen Safety Review and Permitting Process for LNG Facility Proposals (July 19, 2018), https://www.phmsa.dot.gov/news/phmsa-ferc-sign-memorandum-understanding-strengthen-safety-review-and-permitting-process-lng. As a result, the two agencies jointly published a specific, detailed memorandum of understanding (MOU). Memorandum of Understanding Between the U.S. Dep't of Transp. & FERC on Liquefied Natural Gas Transportation Facilities 1 (Aug. 31, 2018), https://www.ferc.gov/sites/default/files/2020-04/FERC-PHMSA-MOU.pdf. This MOU delineates roles and responsibilities over facilities subject to both agencies' oversight, which results in a streamlined and efficient process. *Id.*

124. Given that both agencies have entered into these jurisdictional agreements before, they will likely consider doing the same here. *See* GAO-19-48, *supra* note 31, at 21–22; *supra* note 123 and accompanying text.

125. While the Government Accountability Office recommends that the TSA enhance both its cyber and physical pipeline security measures, *see* GAO-19-48, *supra* note 31, at 61

2. Plan B

In the alternative to the Commission's *sua sponte* statutory reinterpretation, Congress should pass an Act—like the Energy Policy Act of 2005—that expressly gives the Commission authority over pipeline cybersecurity and tasks the Commission with delegating a national natural gas pipeline reliability organization.[126] Lawmakers designed the Energy Policy Act of 2005 to provide regulators the power to develop a stronger energy infrastructure,[127] which is the same policy underlying this recommendation. Additionally, some industry players already anticipate a NERC-like organization being established for natural gas pipelines.[128] Although the current Congress's political divide hinders the prospects of passing new legislation, national security measures have rallied bipartisan support.[129]

B. Designate a Natural Gas Reliability Organization

Following the Commission's grant of authority over interstate natural gas pipelines, the Commission should delegate a natural gas reliability organization. First, the Commission will issue an order on the recommended

("[The] TSA cannot ensure that its guidelines reflect the latest known standards and best practices for physical and cybersecurity[]"), the TSA is more practiced in physical security. *See supra* note 69 and accompanying text.

126. As a federal agency, the "FERC is a 'creature of statute,' having 'no constitutional or common law existence or authority, but only those authorities conferred upon it by Congress.'" Atl. City Elec. Co. v. FERC, 295 F.3d 1, 8 (D.C. Cir. 2002) (emphasis removed) (quoting Michigan v. EPA, 268 F.3d 1075, 1081 (D.C. Cir. 2001)). Although only one bill was introduced last year that would address pipeline cybersecurity, the Pipeline and LNG Facility Cybersecurity Preparedness Act, S. 300, 116th Cong. (2019), additional ranking lawmakers have petitioned Congress to address the current state of cybersecurity standards and agency oversight of pipelines. *See* Letter from Maria Cantwell, Ranking Member, Senate Comm. on Energy & Nat. Res., & Frank Pallone, Jr, Ranking Member, House Comm. on Energy & Com., to Kirstjen Nielson, Sec'y, U.S. Dep't of Homeland Sec. (Dec. 19, 2018), https://www.energy.senate.gov/public/index.cfm?a=files.serve&File_id=ECD424B6-9837-4F1C-BF0A-4FA2BE0FA203.

127. *Energy Policy Act of 2005 Fact Sheet*, FERC (Aug. 8, 2006), https://www.ferc.gov/sites/default/files/2020-04/epact-fact-sheet.pdf (relaying the major impacts of the Act).

128. Siciliano, *supra* note 78 (reporting a legal consultant's belief that, based on discussions with DHS, "the government is aiming for [] something akin to the North American Electric Reliability Corporation").

129. *See Senators Introduce Bipartisan Legislation to Develop American 5G Alternatives to Huawei*, HOMELAND SEC. TODAY (Jan. 14, 2020), https://www.hstoday.us/subject-matter-areas/cybersecurity/senators-introduce-bipartisan-legislation-to-develop-american-5g-alternatives-to-huawei/ (proposing to invest $1 billion to create technology alternatives to Chinese equipment that threatens United States national security and economy).

action—creating a natural gas reliability organization.[130] Interested parties will file comments and responses, FERC staff will recommend an action, and the Commission will issue an order creating the organization.[131] The Commission will follow the same process for developing and approving new mandatory standards.

This proposed natural gas reliability organization would parallel the electricity sector's NERC, further leveling the differences between the electricity and natural gas sectors.[132] The Commission, which has experience forming and overseeing a dedicated reliability organization, would be vested with approval authority over the natural gas reliability organization's proposed cybersecurity standards and penalties.

C. Develop and Enforce Mandatory Cybersecurity Standards for Pipelines

To truly secure America's reliable and consistent flow of energy, pipeline owners and operators must be held to *mandatory* standards that are clearly defined and carry the weight of other similar federal compliance standards.[133] The Commission, along with the natural gas reliability organization, should develop pipeline-specific, mandatory cybersecurity standards through a notice-and-comment period. Utilizing this process will ensure the industry, affected parties, and cybersecurity technical experts have sufficient time to contribute opinions and best practices to create the best possible result.[134] The Commission should propose preliminary standards, consider input to

130. *Rulemaking Process: Notice of Proposed Rulemaking*, FERC, https://www.ferc.gov/media/rule-making-process (last visited Aug. 11, 2020) (describing the FERC rulemaking process).

131. *Id.*

132. The NERC is an international organization spanning Canada, the continental United States, and the northern portion of Baja California, Mexico. *About NERC*, *supra* note 66. Creating an organization to parallel this responsibility in the pipeline sector would further foster national security by protecting pipelines that extend into neighboring countries.

133. *See* Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks that Target and Degrade the Grid*, 40 WM. MITCHELL L. REV. 647, 669–70 (2014) (noting how cybersecurity measures are costly for enterprises to implement and maintain). Therefore, when presented with overlapping yet divergent standards—one set voluntary and the other mandatory with a heavy noncompliance fine—enterprises must make strategic choices. *Id.* (comparing the White House's voluntary cybersecurity initiative and NERC's mandatory standards).

134. Jessica Mantel, *Procedural Safeguards for Agency Guidance: A Source of Legitimacy for the Administrative State*, 61 ADMIN. L. REV. 343, 388 (2009) (suggesting that some public participation in agency decisionmaking may "promote the legitimacy of the administrative state").

develop the final regulation, and enforce these standards as mandatory.[135] Failure to comply with the implemented mandatory standards within twelve months of consummation should result in a monetary penalty.[136]

Debate exists over whether voluntary or mandatory cybersecurity standards are the best way to a more secure energy supply in the United States.[137] Proponents of mandatory standards believe that a regulatory "structure with some teeth" can improve cybersecurity success in the energy industry.[138] In contrast, proponents of voluntary standards find that the pipeline system is tested and has proven itself resilient notwithstanding today's current lack of regulatory requirements.[139] The natural gas industry resents mandatory cybersecurity regulations because "prescriptive rules" are not "suited to address fast-moving cyberthreat."[140] However, it remains unclear how voluntary standards are any better suited to respond to the advanced pace of cyberattacks.

The electricity sector's experience with mandatory standards can provide insight into which approach is likely to improve pipeline security. After regulators imposed mandatory standards on the electricity sector in 2008, electric companies continuously lapsed in compliance, racking up huge monetary fines.[141] If mandatory standards carrying a fine were inadequate to force some electric utilities to comply with NERC CIP Standards, hoping that private pipeline owners will implement voluntary

---

135. After the notice-and-comment period for creating these standards, the Commission's order should include the mandatory nature of the regulations. *See* Trope & Humes, *supra* note 133 (describing the rulemaking process).

136. Echoing the Commission's and NERC's authority in the electricity sector, *see supra* notes 97–98, the Commission can enforce penalties of $1 million per violation, per day, in the natural gas sector. 15 U.S.C. § 717t–1.

137. *See, e.g.*, Dancy & Dancy, *supra* note 25, at 619 (concluding that voluntary standards are best suited for natural gas pipelines).

138. *See* Weber, *supra* note 6 (noting that former Commissioner LaFleur supports mandatory standards and Commissioner Glick believes the TSA does not have the appropriate expertise to regulate pipelines); *see also* Troutman Pepper Pipeline Practice, *supra* note 78 (proposing the promulgation of regulations that specify the standards necessary for protecting pipelines after increases in cybersecurity threats and pipeline sabotage).

139. NAT. GAS COUNCIL, *supra* note 20, at 26 (stating the natural gas industry has robust cybersecurity measures that protect pipelines from disruption); Richard G. Smead, *Weather Resilience in the Natural Gas Industry, The 2017-2018 Test and Results*, RBN ENERGY, LLC. 6 (Aug. 2018), https://drive.google.com/file/d/1gdyLshGFbAOLERXpf4Ss-IemFTfNmUV5/view (finding natural gas pipelines incredibly resilient from weather events).

140. Sobczak, *supra* note 120.

141. *See* Gheorghiu, *supra* note 95.

guidelines issued by the TSA is a lost cause.[142] Making pipelines more secure will inevitably come at a financial cost.[143] Without a federal regulation, for-profit transmission companies are unlikely to implement all necessary recommendations.

As an alternative to punitive monetary fines for noncompliance, the Commission could incentivize the implementation of cybersecurity measures. For example, the Commission could allow utilities to include mandatory cybersecurity measures in their rate base, thereby creating a return on investment.[144]

Mandatory cybersecurity standards do not have to be identical between the electricity and natural gas pipeline sectors. Although increasingly connected, the defining characteristics that lead these two sectors to such traditionally disjointed regulatory approaches still exist and warrant sector-specific cybersecurity approaches. Including the notice-and-comment period will help tailor these new standards to the unique needs and features of the natural gas pipeline industry.[145]

CONCLUSION

In an increasingly connected world and industry, regulators must take a holistic approach to protecting the nation's energy from cyber threats.[146] Because natural gas pipelines and the electricity sector are so dependent on one another, voluntary cyber protections over natural gas pipelines fail to protect both the natural gas and electricity sectors. The Commission should

---

142. *Id.*

143. *See* Trope & Humes, *supra* note 133, at 669 (describing the financial costs associated with pursuing cybersecurity objectives).

144. See Jim Clarkson, *Public Utility Ratemaking 101 (The Problems of Rate Base, Cost Passthrough)*, MASTERRESOURCE (Mar. 24, 2016), https://www.masterresource.org/public-utility-regulation/public-utility-ratemaking-101, for the basic formula used to determine a regulated utility's revenue. Regulated utilities, including natural gas transmission pipelines using a cost-of-service rate, are permitted to recover the cost of providing service (usually operating and maintenance costs) and a reasonable return on their investment. *Id.*; *see also Ratemaking for Energy Pipelines*, AM. GAS ASS'N (2011), https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/Ratemaking%20for%20Energy%20Pipelines%20071111.pdf. In *Kansas City Power & Light Co. v. Missouri Public Service Commission*, 509 S.W.3d 757, 772 (Mo. Ct. App. 2016), although the state public service commission rejected the utility's request to include a specific cybersecurity cost in its revenue requirement, the court did not strike down the utility's attempt to recover a return on investment. Procedural missteps aggravated the utility's opportunity to recover the requested cybersecurity cost. *Id.*

145. *See* Mantel, *supra* note 134, at 388.

146. *See* ENERGY PLAN, *supra* note 14, at 21; *2019 Cybersecurity Awareness Symposium*, *supra* note 105.

reinterpret the scope of its authority under the NGA to exercise regulatory power over interstate natural gas pipeline cybersecurity standards and create a natural gas reliability organization—Plan A. This reinterpretation of the FERC's NGA authority to impose pipeline cybersecurity standards, which would be analogous to its power under the FPA, is in accordance with the Supreme Court's approach to determining the Commission's authority.[147] Additionally, creating a national natural gas reliability organization would benefit the natural gas sector and the energy industry at large. Alternatively, Congress could pass legislation granting the Commission this authority—Plan B. Through either option, an independent agency with the requisite expertise and authority to regulate the energy sector—whether promulgating rules to move energy resources or produce electricity—will improve U.S. national security.

147. *See* FERC v. Elec. Power Supply Ass'n, 136 S. Ct. 760, 766 (2016).