ARTICLE

CYBERSECURING THE PIPELINE

Ido Kilovaty[*]

ABSTRACT

The Colonial Pipeline ransomware attack, which shut down gas supply to the entire East Coast back in May 2021, has sparked the debate as to the regulation of the pipeline's cybersecurity. After ten years of inaction on the matter, the Transportation Security Administration (TSA) has issued two mandatory directives on pipeline cybersecurity. This Article delves into the propriety of the TSA as a pipeline security regulator, as well as the incomplete and ineffective approach currently laid out in the TSA's pipeline cybersecurity directives. This Article argues that there may be other agencies more suitable for the task, such as the Federal Energy Regulatory Commission, acting under the auspices of the Department of Energy. It also provides specific recommendations as to the substance of any prospective pipeline cybersecurity regulation, such as the creation of more open-ended and flexible cybersecurity objectives as opposed to the current approach of prescriptive standards.

[*] Frederic Dorwart and Zedalis Family Fund Endowed Associate Professor of Law, University of Tulsa, College of Law. Affiliate, Northeastern University Law School Center for Law, Innovation, and Creativity. Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School. Affiliate Fellow, Information Society Project, Yale Law School. The Author wishes to thank James Dempsey for his helpful feedback. The Author also wishes to thank the terrific student editors at the *Houston Law Review* who edited this Article, including John Carbonari, Jesús Davila, Matthew Frost, Jake Guarino, Omar Haq, Jessalyn McAlister, Helene Miranda, Haekyong Min, Jack Lenske, Sean O'Leary, Kirsten Hallmark, Michael Dinnella, Robert Clary, Amanda Dorman, Chelsea Ogan, Laura Murray, Olivia Wogon, Chandler Johnson, and Holton Farnum.

TABLE OF CONTENTS

I. INTRODUCTION...607

II. THE PIPELINE: STRUCTURE AND RISKS.........................611
A. *Structure*...611
B. *Risks*...614
1. *Unauthorized Commands and Manipulation.*..615
2. *Delaying or Blocking the Flow of Information.*......................................617
3. *Availability Attacks.*......................................618
C. *Pipeline Insecurity Effects*....................................619
1. *Physical Effects.*..619
2. *National Security Effect.*................................621
3. *Environmental Effects.*...................................623
D. *Responding to the Risks*..623

III. THE REGULATORY LANDSCAPE OF PIPELINE CYBERSECURITY..624
A. *SD-01: Enhancing Pipeline Cybersecurity*...........626
1. *Report.*...626
2. *Assess Practices and Designate a Cybersecurity Coordinator.*............................627
B. *SD-02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*........628
1. *Mitigation Measures*......................................628
2. *Contingency and Response Plan.*...................629
3. *Third-Party Audits.*..629

IV. SHORTCOMINGS OF THE CYBERSECURITY REGULATION OF THE PIPELINE......................................630
A. *The TSA as a Pipeline Cybersecurity Regulator*...631
B. *Information Sharing*...633
C. *Overreliance on Prescriptive Standards*..............635

V. THE PATH FORWARD: SECURING THE PIPELINE...........636
A. *Authorize the Department of Energy to Regulate Pipeline Cybersecurity*........................637
B. *Address the Ransomware Problem*........................640

C. Implement Zero Trust Security Controls 644
D. Rely on Performance-Based Standards for Pipeline Cybersecurity 645
E. Increase Transparency in Pipeline Cybersecurity 646
F. Strengthen the Critical Infrastructure's Cybersecurity 647
G. Set an International Due Diligence Standard 649

VI. CONCLUSION 650

I. INTRODUCTION

On May 7, 2021, Colonial Pipeline, the largest fuel pipeline in the United States, suffered the most significant ransomware attack against U.S. energy infrastructure in history.[1] Its systems had been infected with ransomware, a malicious software that locks systems until a ransom is paid, usually in the form of cryptocurrency.[2] As a result, access to gasoline and jet fuel in the East Coast had been severely limited, and it took several days until Colonial was able to resume normal operation.[3]

The ransomware attack encrypted the files on a billing computer used by Colonial Pipeline, but out of caution, Colonial Pipeline had to shut down its operation technology systems to avoid further disruption and infection with the ransomware.[4] To release the Colonial Pipeline computer systems and networks from

[1] Gloria Gonzalez et al., *'Jugular' of the U.S. Fuel Pipeline System Shuts Down After Cyberattack*, POLITICO (May 8, 2021, 9:29 PM), https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984 [https://perma.cc/GZ87-4EJM]; *About Us*, COLONIAL PIPELINE, https://www.colpipe.com/about-us [https://perma.cc/A665-VKZD] (Oct. 11, 2022).

[2] Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks [https://perma.cc/XKF4-9D6D] (explaining how "Bitcoin and other cryptocurrencies made it possible to extort huge ransoms from large companies, hospitals and city governments").

[3] *Media Statement Update: Colonial Pipeline System Disruption*, COLONIAL PIPELINE, https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption [https://perma.cc/JYV4-Q432] (May 17, 2021, 5:25 PM).

[4] Lily Hay Newman, *Colonial Pipeline Paid a $5M Ransom—and Kept a Vicious Cycle Turning*, WIRED (May 14, 2021, 7:00 AM), https://www.wired.com/story/colonial-pipeline-ransomware-payment/ [https://perma.cc/AF8M-E5YW] ("[T]he company's billing system had been infected with ransomware, so it had no way to track fuel distribution and bill customers.").

the ransomware, hackers demanded a 75 Bitcoin ransom (equivalent to $4.4 million), which Colonial inevitably paid.[5] While Colonial Pipeline was able to restore its operation after the payment, hackers got away with almost 100 gigabytes of sensitive data.[6] This was the most significant ransomware attack against any U.S. critical infrastructure system in history.[7]

The Colonial Pipeline ransomware attack reignited the importance of the energy infrastructure's cybersecurity.[8] Notably, the pipeline's cybersecurity poses a unique challenge compared to the security of the energy infrastructure as a whole, for a variety of reasons that this Article will address.

Indeed, many regulatory initiatives have been made in the Colonial Pipeline attack's aftermath, which in turn exposed the many current shortcomings of the pipeline's cybersecurity regulation in the United States. For example, up until the attack, cybersecurity standards for pipeline companies had been largely voluntary and outdated.[9] The rationale was that it would be in the pipeline owner or operator's best interest to follow these "best practices."[10] The voluntary cybersecurity standards approach is not unique to the pipeline, as the United States has over the years

[5] *See* Michael D. Shear et al., *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (June 7, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/EM34-A496]; William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 2:58 PM), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/5XKU-A64N].

[6] Turton & Mehrotra, *supra* note 5.

[7] Gonzalez et al., *supra* note 1.

[8] *See, e.g.*, *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack: J. Hearing Before the Subcomm. on Cybersecurity, Infrastructure Prot., & Innovation & the Subcomm. on Transp. & Mar. Sec. H.R. of the H. Comm. on Homeland Sec.*, 117th Congress (2021) [hereinafter *Hearing*].

[9] *See, e.g.*, PAUL W. PARFOMAK & CHRIS JAIKARAN, CONG. RSCH. SERV., RL 31340, PIPELINE CYBERSECURITY: FEDERAL PROGRAMS 1 (2021) ("TSA relied on voluntary pipeline cybersecurity guidance and best practices."); TRANSP. SEC. ADMIN., PIPELINE SECURITY GUIDELINES 22–27 (2021); TRANSP. SEC. ADMIN., PIPELINE SECURITY SMART PRACTICE OBSERVATIONS (2011).

[10] Joseph R. Dancy & Victoria A. Dancy, *Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks*, 2 OIL & GAS, NAT. RES., & ENERGY J. 579, 598–99 (2017).

embraced a similar approach in many other critical infrastructure sectors.[11]

However, these voluntary best practices, issued by none other than the Transportation Security Administration (TSA), were no different than any other suggested best practices, such as the one articulated by the Interstate Natural Gas Association of America[12] and the American Petroleum Institute.[13] In other words, up until Colonial Pipeline had been attacked, there was no mandatory cybersecurity regulation for the pipeline sector. Additionally, while the TSA urged Colonial Pipeline to participate in physical and cyber pipeline security assessments prior to the ransomware attack, it did not have any enforcement mechanism for its voluntary guidelines.[14] In short, the pipeline sector's cybersecurity was in effect self-regulated.

In response, the Department of Homeland Security announced that one of its units, the TSA, would update its pipeline cybersecurity approach by issuing mandatory cybersecurity directives for U.S. pipeline companies with the view of preventing future devastating attacks against the pipeline infrastructure.[15]

The TSA's somewhat surprising regulatory authority to deal with the pipeline's cybersecurity is an artifact of the

[11] *See* Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. REV. 515, 517, 534 (2017) ("The United States and some other nations have thus far opted for very light regulation, merely encouraging voluntary steps while choosing to only intervene in a handful of sectors considered decidedly 'critical.'").

[12] *See generally* INGAA, CONTROL SYSTEMS CYBER SECURITY GUIDELINES FOR THE NATURAL GAS PIPELINE INDUSTRY (2011), https://www.aga.org/sites/default/files/legacy-assets/membercenter/gotocommitteepages/NGS/Documents/INGAAControlSystemsCyberSecurityGuidelines.pdf [https://perma.cc/7UYX-WF9M].

[13] *See* Dancy & Dancy, *supra* note 10, at 599; *New Edition of Cybersecurity Standard for Pipelines Provides Comprehensive Approach to Cyber Defense for Critical Infrastructure*, API (Aug. 18, 2021), https://www.api.org/news-policy-and-issues/news/2021/08/18/third-edition-of-api-standard-1164 [https://perma.cc/A9KP-PPVC].

[14] *See Hearing*, *supra* note 8 (statement of Bonnie Watson Coleman, Chairwoman, Subcomm. on Transp. & Mar. Sec.) ("According to TSA, prior to the attack, TSA had asked Colonial Pipeline on no less than 13 occasions to participate in physical and cyber pipeline security assessments. Citing COVID-19, Colonial repeatedly delayed and chose not to participate. On multiple occasions Colonial didn't even bother responding to TSA's e-mails. In fact, Colonial still has not agreed to participate in a physical assessment, and only agreed to cooperate with TSA's cybersecurity assessment 3 weeks after the ransomware attack occurred.").

[15] *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*, U.S. DEP'T HOMELAND SEC. (July 20, 2021) [hereinafter *DHS Announcement*], https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators [https://perma.cc/A2H5-6E6F].

post-9/11 world, whereby the new agency has been tasked with protecting certain infrastructure against potential terrorist attacks.[16] However, given the plethora of cybersecurity threats faced by the energy infrastructure, the TSA's capability of efficaciously ensuring the security of data, computers, networks, and systems running the oil and gas pipelines is doubtful. Already, in 2019, two years before the Colonial Pipeline ransomware attack, the Government Accountability Office (GAO) issued a report where it identified several "weaknesses" with regard to the TSA pipeline security guidelines.[17] These so-called weaknesses are exacerbated by the TSA's lack of expertise and staff to carry out its important role.[18]

This Article addresses the recent pipeline cybersecurity directives issued by the TSA and the debate surrounding the current approach to the pipeline's cybersecurity. It seeks to explore some of these current weaknesses with the TSA regulatory model for pipeline cybersecurity, as well as some broader challenges. This Article takes on a thorny, complex, and often ignored area of cybersecurity regulation—the data and system security of the U.S. energy pipeline network, which consists of three million miles of pipeline, transporting gas, oil, refined products, and other liquids.[19]

This Article makes two main arguments. First, that the TSA may not be the most fitting agency to regulate and enforce pipeline cybersecurity. For reasons that will be discussed in this Article, such as lack of expertise and staff shortage, the TSA needs to be replaced by another agency, such as the Federal Energy Regulatory Commission (FERC), acting under the auspices of the Department of Energy (DOE).

Second, that any pipeline cybersecurity regulations will have to include additional elements on top of the current TSA-issued

[16] Brian Naylor, *Beyond Airports, TSA Also Manages Pipeline Security. That Could Be a Problem*, NPR (May 19, 2021), https://www.npr.org/2021/05/19/997958344/beyond-airports-tsa-also-manages-pipeline-security-that-could-be-a-problem [https://perma.cc/GF83-XAXW] (discussing the TSA authority to regulate pipeline cybersecurity).

[17] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-542T, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT (2019).

[18] *Id.*; Hillary Hellmann, *Acknowledging the Threat: Securing United States Pipeline SCADA Systems*, 36 ENERGY L.J. 157, 168 (2015) ("Neither [the TSA nor DHS] may be sufficiently well-equipped to handle cyber threats without industry aid.").

[19] PARFOMAK & JAIKARAN, *supra* note 9, at 1.

directives. For example, the regulations will have to include more general cybersecurity objectives in addition to the more specific, prescriptive standards currently articulated in the TSA directives.

This Article's contributions are as follows. First, it offers some perspective on what pipeline cybersecurity ought to achieve. Second, it analyzes the recently issued TSA directives, for which there is very little analysis to date in legal scholarship. Third, it highlights the current shortcomings of the existing regulatory approach to raise awareness to the issue among policymakers and other scholars working in this area. Finally, this Article makes specific recommendations to address the current shortcomings of the regulatory approach to pipeline cybersecurity.

This Article proceeds as follows: Part II will provide an overview of the oil and gas pipeline sector and cybersecurity risks. This will serve as a foundation for the discussion in Part III, focused on the current regulatory landscape of pipeline cybersecurity. Part IV will identify the shortcomings of this regulatory approach, related both to the agency involved, the TSA, and the substance of the directives applicable to pipeline cybersecurity. Finally, Part V will propose ways to rethink and modernize the regulatory approach to pipeline cybersecurity, which includes rethinking the TSA's role as a pipeline cybersecurity regulator and ways to fill the gaps in the current cybersecurity regulations.

II. THE PIPELINE: STRUCTURE AND RISKS

The risks faced by the U.S. pipeline infrastructure are not always straightforward.[20] After all, the pipelines are merely conduits for conveying gas, oil, and other hazardous liquids. What exactly are the cybersecurity risks that ought to be regulated in this context? To understand the risks, we need to first lay out the structure of the oil and gas pipeline systems.

A. Structure

The American economy is highly dependent on networks of pipelines carrying a variety of critical products. For petroleum and

[20] *See, e.g.*, OIL & NAT. GAS SUBSECTOR COORDINATING COUNCIL & NAT. GAS COUNCIL, DEFENSE-IN-DEPTH: CYBERSECURITY IN THE NATURAL GAS & OIL INDUSTRY (2018).

gas products, there are approximately 230,000 miles of oil pipelines carrying crude oil and refined petroleum products, and 2.6 million miles of gas pipelines.[21] Largely, these pipelines are privately owned, with a few companies owning "82% of large-diameter pipeline miles and 62% of all pipeline miles in the United States."[22]

Today's pipeline infrastructure is highly computerized and digitized. Pipeline companies operate both information technology (IT) and operational technology (OT) systems.[23] IT comprises regular, day-to-day devices that are used by employees in the course of their job duties, such as laptops, software, and other hardware to facilitate communications.[24] OT, however, is a much more complex and specialized set of industrial control systems that enable cyber-physical capabilities.[25]

One example of an industrial control system (ICS) of concern is a Supervisory Control and Data Acquisition (SCADA) system.[26] A SCADA system is a "computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems."[27] In other words, SCADA comprises the set of computer systems that control actual infrastructure, like

[21] Martin Placek, *Pipeline System Mileage Within the United States from 2004–2020* (Apr. 12, 2022), https://www.statista.com/statistics/197932/us-pipeline-system-mileage-since-2004/ [https://perma.cc/9ZS3-U8QR].

[22] *EIA: Recent Mergers Change the Landscape of Natural Gas Pipeline Ownership*, GAS PROCESSING & LNG, http://gasprocessingnews.com/news/eia-recent-mergers-change-the-landscape-of-natural-gas-pipeline-ownership.aspx [https://perma.cc/2H9M-F6T8] (last visited Sept. 21, 2022).

[23] PARFOMAK & JAIKARAN, *supra* note 9, at 1.

[24] Karen Walsh, *The Colonial Pipeline Attack: Lessons for Enterprise IT*, TECHAERIS (May 13, 2021), https://techaeris.com/2021/05/13/the-colonial-pipeline-attack-lessons-for-enterprise-it/ [https://perma.cc/M8UC-NLDK].

[25] *See* U.S. DEP'T COM., NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBL'N 1500-201, FRAMEWORK FOR CYBER-PHYSICAL SYSTEMS: VOLUME 1, OVERVIEW 1–2 (2017) ("Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use.").

[26] Hellmann, *supra* note 18, at 159, 161 ("Through SCADA, the industry can control thousands of miles of pipeline from one central location. Human controllers can input commands to remotely operate pipeline control equipment.").

[27] *Supervisory Control and Data Acquisition (SCADA)*, NIST, https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition [https://perma.cc/T3FZ-C2TN] (last visited Sept. 12, 2022).

"railways, utility power grids, water and sewer systems, and [the] pipeline networks."[28] They carry out physical processes in the real world. Any compromise of a SCADA system may translate into physical effects, some of which are disruptive and potentially lethal, like explosions and spills.[29]

In the pipeline context, SCADA systems provide an important safety mechanism, which ensures that the infrastructure is operating properly. SCADA systems can generate safety alarms whenever the safety conditions fall outside certain parameters.[30] Targeted SCADA systems may be manipulated into ignoring those unsafe conditions of the infrastructure that they are tasked to operate. This was the case with the Iranian SCADA systems at the nuclear facility in Natanz, which were infected with the Stuxnet malware, causing the centrifuges to spin out of control unbeknownst to the personnel working in the facility.[31]

While SCADA systems raise a multitude of cybersecurity concerns, IT systems may also pose a risk to the normal operation of the pipeline. IT infrastructure can indeed be used to disrupt the pipeline's operations. In fact, Colonial Pipeline shut down its operation to prevent an infected IT system from spreading the ransomware to the ICS.[32]

All in all, the pipeline's systems are vulnerable to cyberattacks, whether they target the IT or ICS of the pipeline operator. Though, the consequences may be different in each case.

[28] Dancy & Dancy, *supra* note 10, at 584.

[29] *Id.* at 585–86 ("[C]yber infiltration of [SCADA] systems could allow successful 'hackers' to disrupt pipeline services and cause spills, explosions, or fires—all from remote locations via the Internet or other communication pathways." (quoting PAUL W. PARFOMAK, CONG. RSCH. SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY 1 (2012))).

[30] *Id.* at 584–85 ("SCADA systems provide the operator with feedback and information about the entire pipeline system and triggers safety alarms when operating conditions are not within the prescribed design parameters. For example SCADA systems monitor pressures, temperatures, tank levels, pump speeds among other variables.").

[31] *See, e.g.*, Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [https://perma.cc/962Q-2PKG]; Christopher M. Bosse, *Stuxnet and Beyond: The Origins of SCADA and Vulnerabilities to Critical Infrastructure*, HOMELAND SEC. TODAY (Dec. 8, 2020), https://www.hstoday.us/federal-pages/dhs/stuxnet-and-beyond-the-origins-of-scada-andvulnerabilities-to-critical-infrastructure/ [https://perma.cc/BCE2-Z6Y4].

[32] Mary Brooks, *IT v. OT: National Security Lessons from Colonial Pipeline*, R ST. (May 12, 2021), https://www.rstreet.org/2021/05/12/it-vs-ot-national-security-lessons-from-colonial-pipeline/ [https://perma.cc/A3XS-W7UK] (explaining that the Colonial Pipeline "shutdown was ordered by the company itself, out of fear that the ransomware might be able to jump from its information technology (IT) networks into the industrial systems").

B. Risks

Given the highly computerized and digitized nature of the pipeline's infrastructure, it faces a myriad of cybersecurity risks that regulators have only lately begun to address. Already back in 2019, the Director of National Intelligence warned in a Worldwide Threat Assessment that the pipeline may be disrupted by foreign actors.[33]

To understand the risks, it is critical to have a solid conception of cybersecurity more generally. Cybersecurity (or information security), generally, seeks to address three main concerns with regard to data, computers, networks, and systems—confidentiality, integrity, and availability. This is often referred to in the information security community as the CIA Triad.[34]

First, confidentiality seeks to ensure that assets are only viewed by authorized parties.[35] For example, a gas company's customer database or proprietary information may only be viewed by specifically designated employees of that company.[36] A breach of confidentiality occurs when a third party, say a rogue hacking organization, gains unauthorized access to the system that stores the secretive data.[37]

Second, "[i]ntegrity refers to the 'ability of a system to ensure that an asset is modified only by authorized parties.'"[38] For example, using the previous example, only an authorized pipeline company employee should be able to modify the company's data or issue specific commands to the ICS. It is a breach of integrity when third parties, say foreign hackers, decide to manipulate the pipeline company's data.[39]

[33] DANIEL R. COATS, DIR. NAT'L INTEL., WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 5 (2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf [https://perma.cc/M8K3-GV7M] ("China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.").

[34] Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, INT'L J. COMPUT. APPLICATIONS ENG'R SCI., July 2011, at 257, 257–58 (2011).

[35] CHARLES PFLEEGER ET AL., SECURITY IN COMPUTING 7 (5th ed. 2015).

[36] *See, e.g.*, *Confidentiality and Proprietary Information.*, ONE GAS, https://ethics.onegas.com/confidentiality-and-proprietary-information [https://perma.cc/L83W-WNCG] (last visited Oct. 14, 2020).

[37] Ido Kilovaty, *Availability's Law*, 88 TENN. L. REV. 69, 77 (2020).

[38] *Id.* (quoting PFLEEGER ET AL., *supra* note 35, at 6).

[39] *Id.*

"And finally, availability pertains to the system's ability to ensure uninterrupted access to assets by authorized users."[40] For example, an oil company's customers should be able to enjoy an uninterrupted flow of service. An availability incident occurs when unauthorized parties target the availability of the system, either by creating bogus traffic that overwhelms the system, which can only handle a limited amount of traffic at single point in time, or by infecting the system with malware that prevents the system from being operational until the incident is resolved.[41]

Now, a ransomware attack is one that compromises both the integrity and availability of a given system. As to integrity, the information encrypted by the ransomware attack is processed through an encryption algorithm that renders it unreadable.[42] This changes the state of information and thus its integrity. In addition, availability is impacted in the sense that the encrypted information or locked system are now inoperable.[43] Even other systems may be inoperable out of caution, as the victim organization seeks to release itself of the ransomware attack.[44] The growing threat of ransomware is magnified by the fact that overwhelmingly, cybersecurity law and policy is concerned with confidentiality rather than integrity and availability.[45]

With the CIA Triad in mind, we can now turn to the specific risks that the pipeline is facing in the context of cybersecurity.

1. Unauthorized Commands and Manipulation. Unauthorized commands transmitted remotely by hackers may change the course of action of the pipeline's ICS.[46] This presents a

[40] *Id.* at 78.

[41] *Id.* at 78, 103.

[42] *See* Josh Fruhlinger, *Ransomware Explained: How It Works and How to Remove It*, CSO (June 19, 2020, 3:00 AM), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html [https://perma.cc/869H-DR9C] (explaining how ransomware encrypts files).

[43] *See CIA Triad*, FORTINET, https://www.fortinet.com/resources/cyberglossary/cia-triad [https://perma.cc/UL86-2NSH] (last visited Sept. 16, 2022) (see under "Availability").

[44] *See, e.g.*, Turton & Mehrotra, *supra* note 5.

[45] Jeff Kosseff, *Defining Cybersecurity Law,* 103 IOWA L. REV. 985, 1024 (2018) ("[C]onfidentiality is an overwhelming focus of many of our cybersecurity laws . . . . However, cybersecurity laws should focus not exclusively on threats to confidentiality, but also on threats to integrity (such as the deletion of important trade secrets or website defacement) and availability (such as denial-of-service attacks).").

[46] *Unauthorized Command Message*, MITRE, https://collaborate.mitre.org/attackics/index.php/Technique/T0855 [https://perma.cc/HE38-QG6J] (last visited Sept. 12, 2022)

real, physical danger to both the infrastructure and people interacting with it or reliant upon it.[47] For example, sending unauthorized commands to the pipeline's infrastructure may result in an increase of the flow of gas, oil, and other liquids to the point of destruction. Conversely, unauthorized commands may also bring the pipelines to a halt, affecting those who rely upon the commodities flowing through the pipes.

This could take place either through the issuance of unauthorized commands or through the manipulation of existing commands and instructions. The National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security acknowledges this concern by laying out the risks, such as "[u]nauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life"[48] and "[i]naccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects."[49]

Some of these risks are illustrated by the 2008 oil pipeline explosion in Turkey, which disabled sensors and alarms, leading to the pipeline catching fire and exploding.[50] While there is still some doubt as to the exact specifics of this pipeline explosion,[51] it nonetheless serves as a cautionary tale as to the potential dangers posed by the pipeline's cybersecurity risks.

("Adversaries may send unauthorized command messages to instruct control system assets to perform actions outside of their intended functionality.").

[47] *Cybersecurity and Physical Security Convergence*, CISA, https://www.cisa.gov/cybersecurity-and-physical-security-convergence [https://perma.cc/EU3V-A27L] (last visited Sept. 15, 2022) ("Together, cyber and physical assets represent a significant amount of risk to physical security and cybersecurity . . . .").

[48] U.S. DEP'T COM., NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBL'N 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY 2 (Rev. 2, 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf [https://perma.cc/2AGW-24RN].

[49] *Id.*

[50] Ariel Bogle, *A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008*, SLATE (Dec. 11, 2014, 5:08 PM), https://slate.com/technology/2014/12/bloomberg-reports-a-cyber-attack-may-have-made-a-turkish-oil-pipeline-catch-fire.html [https://perma.cc/M3WX-YB25].

[51] Robert M. Lee, *Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline*, SANS (June 15, 2015), https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/ [https://perma.cc/4CGG-5B9B].

The risks of unauthorized commands and manipulation are present in other contexts as well. This is a classic example of an integrity attack. However, in the pipeline context, these attacks may result in significant disruption, destruction, and potential significant harm to humans.

2. Delaying or Blocking the Flow of Information. The pipeline's ICS is only properly operational to the extent that it can use the flow of information to carry out the appropriate actions. Certain attacks have the capability to limit or deny completely this important flow of information to the point that the ICS would be unable to carry out the most basic actions.

Delaying or blocking the flow of information may be achieved through a Distributed Denial of Service (DDoS) attack, causing the target to become overwhelmed with traffic to the point of collapse.[52] The majority of oil and gas executives have reported DDoS attacks targeting their SCADA systems.[53] Alternatively, a Man-in-the-Middle attack may similarly control the flow of information between systems.[54] In more extreme cases, a Man-in-the-Middle attack could manipulate commands and messages sent to or between systems.[55]

While delaying, blocking, or otherwise limiting the flow of information to and from SCADA systems may seem mild relative to other methods of attack, it could nonetheless cause severe physical damage. The San Bruno pipeline explosion that killed eight people and injured many others was a result of a glitch in

[52] *See* Josh Fruhlinger, *DDoS Attacks: Definitions, Examples, and Techniques,* CSO (Jan. 31, 2022, 2:00 AM), https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html [https://perma.cc/B6YW-6XWL] (DDoS attacks "work by drowning a system with requests for data . . . . The result is that available internet bandwidth, CPU and RAM capacity becomes overwhelmed.").

[53] Hellmann, *supra* note 18, at 160 ("Distributed Denial of Service (DDoS) attacks are popular. Two-thirds of oil and gas executives reported such intrusions with one-third of industry leaders polled reporting DDoS attacks within their SCADA systems.").

[54] *Man-in-the-Middle Attack (MitM)*, NIST, https://csrc.nist.gov/glossary/term/man_in_the_middle_attack [https://perma.cc/XW3Z-K25Y] (last visited Sept. 15, 2022) ("A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.").

[55] Hellmann, *supra* note 18, at 162.

the SCADA pressure readings.[56] This is but one example out of many where unavailable information has resulted in tragedy.

3. Availability Attacks. Perhaps one of the most important risks that the pipeline is facing is that of availability attacks.[57] Availability attacks may render resources completely unavailable. An example from recent years is ransomware, a type of malware that can disable a system or its data until a ransom is paid.[58] To avoid being traced, hackers often demand a payment in cryptocurrency in exchange for the release of the files or the system.[59]

Colonial Pipeline fell victim to this exact kind of malware. Though, it was not even the OT in Colonial Pipeline's case suffering the ransomware attack, but rather the IT.[60] Regardless, Colonial Pipeline had to shut down its operations, including its OT, until it resolved the situation.[61] Colonial Pipeline was also not the first availability attack against the pipeline sector, as both in 2018 and 2020 certain pipeline operators suffered attacks that disrupted their ability to provide service.[62]

Availability attacks against the pipeline may cause disruptive effects throughout the economy. For example, "[m]inor disruptions may result in increased prices for gasoline, diesel fuel, home heating oil, and natural gas."[63] In more extreme cases, "disruptions could manifest themselves as widespread energy shortages and the inability to produce products such as plastics, pharmaceuticals, and many chemicals that rely on oil and natural gas."[64]

[56] *See* Madeline Labovitz, *Your Natural Gas Is Not Cyber-Secure: A Two-Fold Case for Why Voluntary Natural Gas Pipeline Cybersecurity Guidelines Should Become Mandatory Regulations Overseen by the Department of Energy*, N.C. J.L. & TECH., Mar. 2020, at 217, 229; Dancy & Dancy, *supra* note 10, at 585–86.

[57] *See* Kilovaty, *supra* note 37, at 74 n.28, 102–03 (explaining how availability attacks are "incidents that solely affect the availability of data and systems . . . . [A]vailability attacks are concerned primarily with disruptions of computer systems, networks, and data.").

[58] Fruhlinger, *supra* note 42.

[59] *See* Myre, *supra* note 2.

[60] David Jones, *Colonial Pipeline Disconnects OT Systems to Silo Ransomware IT Threat*, CYBERSECURITY DIVE (May 12, 2021), https://www.cybersecuritydive.com/news/colonial-pipeline-OT-IT-ransomware/600046/ [https://perma.cc/L9JS-JUXR].

[61] *See* PARFOMAK & JAIKARAN, *supra* note 9, at 3.

[62] *See* Don C. Smith, *Cybersecurity in the Energy Sector: Are We Prepared?*, 39 J. ENERGY & NAT'L. RES. L. 265, 268 (2021).

[63] TRANSP. SEC. ADMIN., PIPELINE SECURITY AND INCIDENT RECOVERY PROTOCOL PLAN 3 (2010).

[64] *Id.*

C. Pipeline Insecurity Effects

The manifestation of the aforementioned risks may result in a variety of serious effects that are worth understanding in the context of pipeline cybersecurity. These effects go beyond the immediate and more straightforward digital effects to the affected systems.

First, there are physical effects. The pipeline experiencing a cyberattack may cause serious damage to both the digital and nondigital assets.[65] The physical effects are not limited to property, as individuals may suffer minor or major injuries, and in more rare cases, death, in particular where hazardous, combustible, and toxic liquids or gasses are involved.[66]

Second, an exploited pipeline insecurity may also cause national security effects.[67] Foreign adversaries are increasingly seeking exploitable vulnerabilities in U.S. critical infrastructure.[68] In fact, the United States itself has been engaged in probing and allegedly attacking infrastructure abroad.[69] This raises questions of national and international security.

Third, the unique characteristic of the pipeline as a conduit of hazardous, flammable liquids could lead to serious environmental effects. A pipeline exploding and leaking hazardous liquids or gasses is a concerning environmental effect.

1. Physical Effects. Exploiting vulnerabilities in the pipeline's systems may result in physical effects. The Stuxnet worm, which infected the nuclear facilities in Netanz, Iran, back in 2010, illustrates the ability of malware to cause significant,

[65] Scott D. Applegate, *The Dawn of Kinetic Cyber*, 5th INT'L CONF. CYBER CONFLICT (2013) ("Kinetic cyber attacks are a real and growing threat that is generally being ignored as unrealistic or alarmist.").

[66] *See* David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html [https://perma.cc/7YFZ-LCXR] ("We are talking about the risk of injury or death, not just losing your email.").

[67] *See* Yonatan Striem-Amit, *Cybersecurity Is National Security*, CYBEREASON (Sept. 21, 2021), https://www.cybereason.com/blog/cybersecurity-is-national-security [https://perma.cc/L3V2-VWY2].

[68] *See, e.g.*, Tim Starks, *U.S. Says Russian Hackers Targeted American Energy Grid*, POLITICO, https://www.politico.com/story/2018/03/15/dhs-fbi-russia-hackers-targeted-energy-grid-813745 [https://perma.cc/WL3H-XVWM] (Mar. 15, 2018, 7:46 PM).

[69] David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html [https://perma.cc/YLU8-XDJT].

devastating physical damage to infrastructure.[70] Stuxnet manipulated the SCADA systems to ignore the dangerous speed levels at which the centrifuges had been spinning.[71] Spinning out of control, the centrifuges were irreversibly damaged without any emergency system flagging the unusual behavior.[72]

Stuxnet is not the only cautionary tale on the potential physical effects resulting from a cyberattack. In 2008, the Turkish oil pipeline experienced a cyberattack that resulted in a fiery explosion of the pipeline. The attackers targeted an alarm management network, disabling its operation.[73] Other SCADA error-related pipeline explosions and spills that resulted in the loss of life and damage to property include the San Bruno pipeline explosion[74] and the 1999 Bellingham pipeline rupture.[75] These incidents can be traced as far back as 1982, when the 1982

[70] Zetter, *supra* note 31 ("Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.").

[71] William Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html [https://perma.cc/CB28-JXRJ] (The Stuxnet worm "was designed to send Iran's nuclear centrifuges spinning wildly out of control").

[72] *Id.* ("The computer program also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators . . . so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart.").

[73] Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG (Dec. 10, 2014), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar [https://perma.cc/SBV4-TTVP] ("The central element of the attack was gaining access to the operational controls to increase the pressure without setting off alarms. Because of the line's design, the hackers could manipulate the pressure by cracking into small industrial computers at a few valve stations without having to hack the main control room.").

[74] Dan Weikel, *San Bruno Pipeline Explosion: 'A Failure of the Entire System,'* L.A. TIMES (Aug. 30, 2011, 12:00 AM), https://www.latimes.com/local/la-xpm-2011-aug-30-la-me-0831-san-bruno-20110831-story.html [https://perma.cc/99VL-FY3D] (explaining that the explosion "killed eight people and destroyed 38 homes in the Bay Area last year").

[75] Derek Moscato, *The Lessons of Bellingham's Olympic Pipeline Explosion*, SEATTLE TIMES (June 4, 2019, 2:41 PM), https://www.seattletimes.com/opinion/the-lessons-of-bellinghams-olympic-pipeline-explosion/ [https://perma.cc/NR7B-CZJJ] (describing how the explosion killed three people); MARSHALL ABRAMS & JOE WEISS, BELLINGHAM, WASHINGTON, CONTROL SYSTEM CYBER SECURITY CASE STUDY 8 (2008), https://icscsi.org/library/Documents/Case_Studies/Case%20Study%20-%20NIST%20-%20Olympic%20Pipeline.pdf [https://perma.cc/QK8R-KFH9].

Trans-Siberian pipeline exploded due to a malicious code in its software.[76]

2. National Security Effect. Cyberattacks are not bound by geographical boundaries, which leads to potential national security implications.[77] The Colonial Pipeline ransomware attack was carried out by the Russian hacking group, REvil,[78] some members of which have been recently arrested in Russia as a result of a negotiation between the two countries.[79] As will be discussed later in this Article, this type of international cooperation is essential to address the transnational cybercrime threat to pipeline infrastructure.[80] Russia is by no means the only foreign actor potentially threatening the stability of the U.S. critical infrastructure.[81]

Cyberattacks against critical infrastructure in general, and the pipeline specifically, are attractive for foreign actors trying to destabilize a nation, destabilize its economy, or profit off the many vulnerabilities in the IT, OT, and ICS of critical infrastructure targets.[82] The 2015 Ukraine blackout attack, in which Russia

[76] John Markoff, *A Code for Chaos*, N.Y. TIMES (Oct. 2, 2010), https://www.nytimes.com/2010/10/03/weekinreview/03markoff.html [https://perma.cc/7LG2-WC8G] (describing the first known computer attack in history, in which the Trans-Siberian pipeline explosion caused by the United States sabotaging the Canadian software purchased by Russia).

[77] Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1510 (2013).

[78] Brian Krebs, *At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates*, KREBS ON SECURITY (Jan. 14, 2022, 5:41 PM), https://krebsonsecurity.com/2022/01/at-request-of-u-s-russia-rounds-up-14-revil-ransomware-affiliates/ [https://perma.cc/H687-RDFV].

[79] Maggie Miller, *Russia Arrests Hacker in Colonial Pipeline Attack, U.S. Says*, POLITICO (Jan. 14, 2022, 6:12 PM), https://www.politico.com/news/2022/01/14/russia-colonial-pipeline-arrest-527166 [https://perma.cc/RTG6-7KY7].

[80] *See infra* Section V.G.

[81] *See* COATS, *supra* note 33, at 5 ("*Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners*. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.").

[82] Jeh Charles Johnson, *Cyberattacks on Our Energy Infrastructure: The Need For a National Response to a National Security Threat*, ENERGY SOURCE: ATLANTIC COUNCIL (Dec. 13, 2021), https://www.atlanticcouncil.org/blogs/energysource/cyberattacks-on-our-energy-infrastructure/ [https://perma.cc/R6SD-EQLL]; NAT'L SEC. AGENCY & CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, PP-22-1413, CONTROL SYSTEM DEFENSE: KNOW THE OPPONENT 2–3 (2022) https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA_ICS_Know_the_Opponent_.PDF [https://perma.cc/W232-ULTM].

targeted the electric grid in western Ukraine,[83] with another attack causing a blackout in Kiev in 2016,[84] resulted in a significant disruption to the electricity sector. This threat is of concern in other nations as well, in particular in the United States, where the electric grid has been probed by Russia for vulnerabilities.[85]

Part of the national security concern is also attributed to the psychological effect of cyberattacks against critical infrastructure.[86] This psychological effect is well documented, as the public panic immediately after Colonial Pipeline has demonstrated.[87] Some research shows a broader psychological effect—mental and emotional harm—resulting from cybersecurity incidents.[88]

Any new pipeline cybersecurity regulations will have to address the national security aspect of cyberattacks against the pipeline infrastructure. These regulations are needed not only because of the potential physical effects but also because foreign governments may exploit pipeline vulnerabilities for political and strategic gain.[89]

[83] Dustin Volz, *U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage*, REUTERS, Feb. 25, 2016, 5:52 PM, https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K [https://perma.cc/Y98G-CF28].

[84] Pavel Polityuk et al., *Ukraine's Power Outage Was a Cyber Attack: Ukrenergo*, REUTERS, Jan. 18, 2017, 5:06 AM, https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA [https://perma.cc/75HS-PBW5].

[85] David Gilbert, *Russian Hackers Are Still Probing America's Critical Power Grid Infrastructure*, VICE (Dec. 21, 2018, 9:55 AM), https://www.vice.com/en/article/9k4dbp/russian-hackers-are-still-probing-americas-critical-power-grid-infrastructure [https://perma.cc/MKA9-9EKS].

[86] *See* Haber & Zarsky, *supra* note 11, at 521 ("[A]ttacks against CIs [critical infrastructures] could have a powerful psychological effect on society. Therefore, adversaries have a publicity incentive to attack them and enhance their visibility and prestige.").

[87] *See* Joe R. Reeder & Tommy Hall, *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, CYBER DEF. REV., Summer 2021, at 25 ("[G]as prices at some pumps reached levels not seen since 2008, then pumps ran dry at over 12,000 gas stations across the southeastern US as the panic-buying frenzy as consumers broadened their search radius for fuel.").

[88] *See* Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J.L. & TECH. 1, 4 (2021) ("The mental and emotional impact on consumers has been increasingly studied and documented in recent years.").

[89] Rebecca Beitsch, *DHS Warns Russia Could Launch Cyberattack on US*, HILL, https://thehill.com/policy/national-security/591074-dhs-warn-russia-could-launch-cyberattack-on-us/ [https://perma.cc/7ZM4-ETCF] (Jan. 24, 2022, 2:37 PM) ("Russia has a number of cyber tools it could use to attack the U.S., ranging from 'low-level denials-of-service to

3. Environmental Effects. Cyberattacks against the infrastructure may also lead to harmful environmental effects. The risks of compromised pipeline ICS include "explosions, spills, or fires, which easily will threaten . . . the environment."[90] The 2008 Turkish pipeline explosion, resulting in "30,000 barrels of oil spilled above a water aquifer," is one example of the possible environmental consequences of cyberattacks targeting the pipeline.[91]

While not a petroleum pipeline, the Maroochy Shire cyberattack demonstrated the potential environmental impact of compromised pipelines.[92] The hacker in the Maroochy Shire cyberattack used a wireless system to gain access to the Maroochy sewage system.[93] This hacker caused 800,000 liters of raw sewage to spill into local parks and rivers.[94]

Pipeline cybersecurity standards will have to make the proper balancing between environmental concerns, cybersecurity risks, and the burden of regulation on privately owned pipelines. This also raises the question of negative externalities, which are common in data breach cases.[95] While this is not an easy task by any means, it is crucial that these concerns be accounted for.

D. Responding to the Risks

The Colonial Pipeline ransomware attack illustrated just one out of many risks faced by the pipeline infrastructure. The cybersecurity regulation of the pipeline has become a dynamic, active, and important topic as of late, precisely because of the materialized risk experienced by Colonial Pipeline.

destructive attacks targeting critical infrastructure.'" (quoting DEP'T HOMELAND SEC., NATIONAL TERRORISM ADVISORY BULLETIN (Jan. 23, 2022))).

[90] 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 [https://perma.cc/D8AW-G53L] (quoting Andrew R. Lee, cybersecurity expert, Jones Walker in New Orleans).

[91] Hellmann, *supra* note 18, at 165.

[92] *See generally* Jill Slay & Michael Miller, *Lessons Learned from the Maroochy Water Breach*, *in* 253 CRITICAL INFRASTRUCTURE PROTECTION 73 (IFIP International Federation for Information Processing, Eric Goetz & Sujeet Shenoi eds., 2008).

[93] MARSHALL ABRAMS & JOE WEISS, MALICIOUS CONTROL SYSTEM CYBER SECURITY ATTACK CASE STUDY—MAROOCHY WATER SERVICES, AUSTRALIA 4 (2008), https://apps.dtic.mil/sti/pdfs/AD1107275.pdf [https://perma.cc/F5KB-RHUB].

[94] *Id.* at 1.

[95] Sales, *supra* note 77, at 1520 ("If a company suffers an intrusion, much of the harm will fall on third parties; the attack results in a negative externality.").

Despite the many efforts to respond to the risks and threats against the pipeline, there is still a great deal of uncertainty and incompleteness when it comes to the emerging regulatory responses. However, even with a more serious reform of the pipeline cybersecurity structure and substance, silver bullet solutions for cybersecurity risks rarely exist.[96] Nor is it possible to prevent all cyberattacks indefinitely.[97]

This Article proceeds by laying out the regulatory landscape of pipeline cybersecurity.

III. THE REGULATORY LANDSCAPE OF PIPELINE CYBERSECURITY

Up until the Colonial Pipeline ransomware in May 2021, there had been little to no regulation of the U.S. pipeline.[98] Under the Aviation and Transportation Security Act, establishing the TSA, the TSA has the "security responsibilities over . . . modes of transportation that are exercised by the Department of Transportation," which include the pipeline.[99]

In 2010, based on a statute authorizing the TSA to promulgate regulations for pipeline cybersecurity, the TSA issued the "Pipeline Security and Incident Recovery Protocol Plan," a guidance for the private pipeline sector seeking to prevent, respond to, and recover from cyberattacks.[100] This guidance has been voluntary, meaning that the pipeline sector self-regulated its cybersecurity.[101]

In 2018, given vast cybersecurity threats against critical infrastructure and the private sector, Congress created the Cybersecurity and Infrastructure Security Agency (CISA), which

[96] David Emm, *There Is No Cybersecurity Silver Bullet*, TECH RADAR (June 26, 2020), https://www.techradar.com/news/there-is-no-cybersecurity-silver-bullet [https://perma.cc/5QCG-WHLT].

[97] Sales, *supra* note 77, at 1511 ("[T]he goal [of cybersecurity regulation] is to achieve an efficient level of attacks, not to prevent all attacks.").

[98] Ari Natter & Jennifer A. Dlouhy, *U.S. to Step Up Pipeline Cyber Rules in Wake of April Hack*, BLOOMBERG (July 19, 2021, 9:47 AM), https://www.bloomberg.com/news/articles/2021-07-19/new-cybersecurity-regulations-for-pipelines-set-to-be-released [https://perma.cc/D9ZG-BCMX] (explaining that cybersecurity regulation "until now had relied on self-reporting and other voluntary measures").

[99] 49 U.S.C. § 114(d)(2), (s)(1).

[100] TRANSP. SEC. ADMIN., PIPELINE SECURITY AND INCIDENT RECOVERY PROTOCOL PLAN 1–6 (2010).

[101] Jim Dempsey, *Regulatory Alchemy: Turning Cybersecurity Guidelines into Rules*, LAWFARE (June 1, 2021, 1:30 PM), https://www.lawfareblog.com/regulatory-alchemy-turning-cybersecurity-guidelines-rules [https://perma.cc/D7DY-VHX2].

was tasked with working with other stakeholders and agencies to protect cyber infrastructure from cyberattacks.[102] TSA, in response, issued a "Cybersecurity Roadmap," where it committed to working with CISA on pipeline cybersecurity.[103]

Shortly after the Colonial Pipeline attack, the TSA announced that it would come up with new cybersecurity requirements for critical pipeline owners and operators.[104] The TSA has now issued two binding directives to address pipeline cybersecurity.

The first directive, SD-01, requires that pipeline owners and operators report cybersecurity incidents to CISA, designate a Cybersecurity Coordinator to be available at all times, review current practices, and report any gaps and related remediation measures to TSA and CISA.[105]

The second directive, SD-02, which has not been made public but was obtained through a Freedom of Information Act (FOIA) request,[106] is focused on requiring specific safeguards to protect the IT and OT against known cyberattacks, like ransomware.[107] This directive requires that pipeline operators and owners "implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review."[108]

This part proceeds by providing a detailed account of the two directives, SD-01 and SD-02. These directives are certainly a slight improvement when compared to the pre-Colonial Pipeline voluntary approach; however, many challenges still exist.

[102] *See generally* 6 U.S.C. § 652 (articulating the duties of the Cybersecurity and Infrastructure Security Agency and its personnel).

[103] TRANSP. SEC. ADMIN., TSA CYBERSECURITY ROADMAP 2018 (2018).

[104] *DHS Announcement*, *supra* note 15.

[105] TRANSP. SEC. ADMIN., SEC. DIRECTIVE PIPELINE-2021-01B, ENHANCING PIPELINE CYBERSECURITY (2021) [hereinafter SD-01B].

[106] Aaron Schaffer, *Cybersecurity Experts Have Mixed Reviews of TSA's New Pipeline Rules*, WASH. POST (Oct. 4, 2021, 7:23 AM), https://www.washingtonpost.com/politics/2021/10/04/cybersecurity-experts-have-mixed-reviews-tsa-new-pipeline-rules/ [https://perma.cc/96NL-HV4A].

[107] *DHS Announcement*, *supra* note 15.

[108] *Id.*

A. SD-01: Enhancing Pipeline Cybersecurity

SD-01 is primarily an information sharing directive that requires certain pipeline operators to implement three actions.[109] First, that any cybersecurity incident affecting the pipeline systems be reported to CISA.[110] Second, that every pipeline owner or operator designate a Cybersecurity Coordinator, to be available to the TSA and CISA at all times.[111] Third, that pipeline owners and operators review their systems against TSA's pipeline cybersecurity recommendations and report to the TSA and CISA on any cyber risks, gaps, and remediation measures.[112]

1. Report. Pipeline operators and owners are required under SD-01 to report any cybersecurity incident involving pipeline systems to CISA.[113] These incidents include but are not limited to: unauthorized access to pipeline IT or OT, discovery of malware on pipeline IT or OT, DDoS against pipeline IT or OT, a physical attack on network infrastructure, and any other cybersecurity incident that results in operational disruption or has the potential to cause operational disruption.[114]

The incident report to CISA must also include specific details, such as the affected hazardous liquid or natural gas pipeline, a description of the incident, threat, or activity, and a description of responses to the incident.[115] SD-01 defines a "Cybersecurity Incident" as:

> [A]n event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity

[109] SD-01B, *supra* note 105, at 1–2.
[110] *Id.* at 1.
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.* at 2–3.
[115] *Id.* at 3–4.

> incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).[116]

The definition may seem confusing and somewhat redundant. It requires an "investigation or evaluation by the owner/operator as a possible cybersecurity incident" without determination as to the root and notes that it may affect the "integrity, confidentiality, and availability" of the systems, which is already required at the beginning of the definition.[117]

In comparison to other incident reporting statutes, this definition seems needlessly complex. For example, the FERC definition of a "Cybersecurity Incident" is "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."[118] Though, only a successful malicious act or suspicious event are reportable.[119]

2. Assess Practices and Designate a Cybersecurity Coordinator. SD-01 also requires a vulnerability assessment,[120] in which pipeline owner and operators review their current cybersecurity practices against the latest TSA Pipeline Security Guidelines.[121] The assessment is focused on addressing existing cyber risks, identification of any gaps, and remediation measures to fill the gaps.[122]

To ensure the implementation of SD-01, the directive requires that pipeline operators and owners designate a Cybersecurity Coordinator.[123] The directive lays out the specific prerequisites for any Cybersecurity Coordinator hired by a pipeline company, such as eligibility for security clearance, to be accessible to the TSA and CISA, to coordinate cyber and related security practices and

[116] *Id.* at 5.

[117] *Id.*

[118] Cyber Security Incident Reporting Reliability Standards, 83 Fed. Reg. 36727, 37629 (July 31, 2018) (to be codified at 18 C.F.R. pt. 40).

[119] *Id.*

[120] *Id.* at 36728.

[121] *See generally* SD-01B, *supra* note 105, at 4 (containing the procedures and policies enforced by the TSA to protect pipeline security).

[122] *Id.*

[123] *Id.* at 1.

procedures internally, and more.[124] In similar fashion, the directive also contains the details to be included in every incident report communicated to CISA, such as the hazardous liquid and natural gas pipeline facility affected, a description of the threat, incident, or activity, and a description of responses to the incident.[125] The incident reporting rules cover incidents against both pipeline IT and OT.[126]

Noteworthy is the applicability of SD-01. The main question is which pipeline owners and operators are bound by the directive's rules? SD-01 defines "Owner/Operator" as one who "has been identified by TSA as one of the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations."[127] This seems not to apply to anyone not designated by the TSA as such, such as smaller pipeline owners and operators.

B. SD-02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing

SD-02 forms the bulk of the current pipeline cybersecurity regulations in that it contains the actual substance of what pipeline cybersecurity ought to look like. Notably, the TSA did not make available to the wider public the specific security measures, as it considers them "sensitive security information," though the *Washington Post* was able to obtain a copy by filing a FOIA request.[128]

1. Mitigation Measures. First, SD-02 requires specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems.[129] These are not listed in SD-02's public

[124] *Id.* at 2.

[125] *Id.* at 3–4.

[126] *Id.* at 2.

[127] *Id.* at 6.

[128] Schaffer, *supra* note 106.

[129] *See generally* TRANSP. SEC. ADMIN., SEC. DIRECTIVE PIPELINE-2021-02C, PIPELINE CYBERSECURITY MITIGATION ACTIONS, CONTINGENCY PLANNING, AND TESTING (2022) [hereinafter SD-02C] (containing the specific procedures pipeline owners and operators must establish to protect their information and operation technology systems).

version per the "Nondisclosure of Security Activities" privilege.[130] Typically, these mitigation measures are based on CISA alerts published in response to ongoing global cybersecurity threats and incidents, such as the Ukraine blackout cyberattack of 2015.[131] An example of a mitigation measure includes exercising an incident response plan and disconnecting systems from the internet if such connection is not necessary for the pipeline's operation.[132] Some other measures required by SD-02 are multifactor authentication for nonservice accounts, network segmentation, and retention policies.[133]

2. Contingency and Response Plan. SD-02 also requires the implementation of a cybersecurity contingency/response plan.[134] In the pipeline sector, having a plan B is critical to ensure normalcy in the supply of gas and oil. Indeed, cybersecurity experts reacting to SD-02 have expressed their approval for the requirement of developing and testing an incident response plan.[135]

Under the contingency and response plan, an infected pipeline system needs to be isolated and disconnected as soon as possible.[136] If done correctly, this would prevent further infection of other IT and OT systems on the same network.

3. Third-Party Audits. For the first time ever, an official cybersecurity regulation has mandated an annual cybersecurity audit from either the TSA or a third-party independent inspector,

[130] 49 U.S.C. § 114(r) ("NONDISCLOSURE OF SECURITY ACTIVITIES.— (1) IN GENERAL.—Notwithstanding section 552 of title 5, the Administrator shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107–71) or under chapter 449 of this title if the Administrator decides that disclosing the information would— (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation.").

[131] Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/SEL9-EBDV].

[132] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, ALERT (AA20-205A), NSA AND CISA RECOMMEND IMMEDIATE ACTIONS TO REDUCE EXPOSURE ACROSS OPERATIONAL TECHNOLOGIES AND CONTROL SYSTEMS (2020), https://www.cisa.gov/uscert/ncas/alerts/aa20-205a [https://perma.cc/K8KR-B335].

[133] SD-02C, *supra* note 129, at 5–6, 18.

[134] *Id.* at 8–9.

[135] Schaffer, *supra* note 106.

[136] SD-02C, *supra* note 129, at 8.

which is certainly an important step in the right direction.[137] SD-02 requires that pipeline operators and owners conduct an annual audit of the cybersecurity of their systems by an independent third party.[138]

Yet, with regard to other portions of SD-02, experts expressed some concerns.[139] As will be discussed below, the measures are largely prescriptive, which is not necessarily a sound approach to cybersecurity.[140] For example, requiring the patching of vulnerabilities or the use of anti-virus software scans does not address the underlying cybersecurity goals with the use of these measures.[141]

IV. SHORTCOMINGS OF THE CYBERSECURITY REGULATION OF THE PIPELINE

Acknowledging the gap in pipeline cybersecurity regulation is a welcome step in the right direction; however, the TSA model of regulating the pipeline's cybersecurity suffers from a multitude of weaknesses.

First, there is the issue of expertise. Is the TSA the appropriate entity to regulate the pipeline's cybersecurity, given that the TSA lacks expertise in the areas necessary for an efficient regulatory regime?[142] This Article argues that the TSA is not the proper agency through which the pipeline's cybersecurity may be regulated.

Second, assuming the TSA remains the primary regulator of the pipeline's cybersecurity, the contents of the regulations need to be scrutinized. Currently, the TSA's approach to regulating the pipeline's cybersecurity is inadequate, incomplete, and outdated.

This part proceeds in three sections. First, it discusses the TSA as a pipeline cybersecurity regulator, with the many challenges attached to that role and the realities of the TSA as a noncyber agency. Second, the TSA's and other agencies'

[137] *Id.* at 9–10.

[138] *Id.* at 9.

[139] Schaffer, *supra* note 106.

[140] *See infra* Section IV.C.

[141] SD-02C, *supra* note 129, at 7–8.

[142] Robert K. Knake, *The TSA Should Regulate Pipeline Cybersecurity*, COUNCIL ON FOREIGN RELS.: NET POL. (May 10, 2021, 5:45 PM), https://www.cfr.org/blog/tsa-should-regulate-pipeline-cybersecurity [https://perma.cc/9TUX-67L2] ("Congress should also act on an emergency basis to fund the TSA's Pipeline Security Program, which is woefully understaffed and historically lacks the requisite expertise.").

information sharing approach needs to be supplemented by more robust cybersecurity measures. Third, the TSA's overreliance on prescriptive standards is misguided. It will need to be complemented by performance-based standards.

A. *The TSA as a Pipeline Cybersecurity Regulator*

The TSA has been criticized for lacking the expertise and tools needed to effectively regulate cybersecurity in the pipeline context.[143] For example, it was unclear whether the TSA sufficiently consulted industry stakeholders when promulgating its directives[144] or whether it even has the expertise to come up with an effective cybersecurity regulation regime.[145] Some have also criticized the TSA and CISA for promulgating directives under emergency authority, which allowed them to forego industry input through the traditional process of rulemaking.[146] The draft directive has also not been made available to Congress at any point.[147]

As another example, while the TSA based its security guidelines on NIST's Framework for Improving Critical Infrastructure Cybersecurity,[148] the guidelines miss many elements

[143] Madeline A. Labovitz, Note, *Your Natural Gas Is Not Cyber-Secure: A Two-Fold Case for Why Voluntary Natural Gas Pipeline Cybersecurity Guidelines Should Become Mandatory Regulations Overseen by the Department of Energy*, 21 N.C. J.L. & TECH. 217, 254 (2020) ("TSA is not the agency that should promulgate mandatory regulations—the agency simply does not have the necessary resources, nor expertise.").

[144] Mariam Baksh, *Biden Official Endorses Effort to Move Pipeline Cybersecurity Regulation to DOE*, NEXTGOV (Jan. 19, 2022), https://www.nextgov.com/cybersecurity/2022/01/biden-official-endorses-effort-move-pipeline-cybersecurity-regulation-doe/360915/ [https://perma.cc/3MH2-WCSH].

[145] Ellen Nakashima & Lori Aratani, *DHS To Issue First-Ever Cybersecurity Regulations for Pipelines After Colonial Hack*, WASH. POST (May 25, 2021), https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/ [https://perma.cc/7WB8-VZBF].

[146] Letter from Rob Portman, James Lankford, and M. Michael Rounds to Joseph V. Cuffari, Inspector General, Dep't Homeland Sec. (Oct. 28, 2021) [hereinafter Letter to Joseph Cuffari], https://www.hsgac.senate.gov/imo/media/doc/2021-10-28%20RP%20Lankford%20Rounds%20to%20Cuffari%20re%20TSA%20Security%20Directives.pdf [https://perma.cc/RR4V-BKKQ] ("[W]e have received reports that TSA and CISA failed to give adequate consideration to feedback from stakeholders and subject matter experts who work in these fields and that the requirements are too inflexible.").

[147] *Id.*

[148] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-542T, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT (2018), https://www.gao.gov/assets/gao-19-542t.pdf [https://perma.cc/VR9S-HLRP] ("However, TSA's revisions do not include all elements of the current [NIST] framework and TSA does not have a documented process for reviewing and revising its guidelines on a regular basis.").

from the Cybersecurity Framework, which makes the TSA security guidelines incomplete and inadequate in addressing the cybersecurity threats against the pipeline.[149] The NIST Cybersecurity Framework is important, for example, because it creates a "common language" for cybersecurity and promotes collaboration between private companies,[150] which is critical for pipeline cybersecurity.[151]

The GAO noted that the TSA has no process for reviewing and revising its guidelines, and therefore, the TSA "cannot ensure that its guidelines reflect the latest known standards and best practices for physical and cybersecurity, or address the persistent and dynamic security threat environment [that pipelines face]."[152]

Also notable is the TSA's shortage in human capital necessary to carry out its pipeline cybersecurity mission.[153] The TSA employed fourteen full-time employees working on pipeline cybersecurity in fiscal years 2012 and 2013, one employee in 2014, and merely six employees in 2018.[154] In 2019, the TSA employed five full-time pipeline security employees, none with cybersecurity expertise.[155] The TSA has previously acknowledged that it lacks the personnel to fully perform its pipeline cybersecurity mission.[156]

Finally, pipeline operators and industry members reported that the TSA seems to lack the requisite expertise to regulate the pipeline's cybersecurity.[157] This lack of expertise and staff shortage has led to an inability to conduct the very critical security reviews of pipeline cybersecurity, Corporate Security Reviews (CSRs) and Critical Facility Security Reviews.[158]

Currently, there are some tensions between the TSA and the FERC, an entity within the DOE responsible for the electric

[149] *Id.* at 32–33.

[150] Hellmann, *supra* note 18, at 171–72.

[151] *Id.*

[152] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-48, CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT 33 (2018) [hereinafter GAO REPORT 19-48], https://www.gao.gov/products/gao-19-48 [https://perma.cc/WSK9-NEEM].

[153] *Id.* at 37–38.

[154] PARFOMAK & JAIKARAN, *supra* note 9, at 13.

[155] *Id.* at 15.

[156] *Id.* at 14.

[157] *Id.* at 13 ("Pipeline operators and industry representatives reported that TSA lacked the expertise required to fully assess cybersecurity in security reviews. TSA did not, at the time, have a strategic workforce plan that identified staffing needs and skill sets such as cybersecurity.").

[158] GAO REPORT 19-48, *supra* note 152, at 37.

sector's cybersecurity regulation. Two FERC commissioners have expressed their concern as to the adequacy of the TSA as a pipeline cybersecurity regulator.[159] Their observation included a call for a different agency to regulate pipeline cybersecurity, one that "fully comprehends the energy sector and has sufficient resources to address this growing threat."[160] In the same vein, the Biden Administration announced its support to move pipeline cybersecurity from the TSA to the FERC.[161] Certain House representatives even proposed the Energy Product Reliability Act to allow the FERC to regulate the pipeline's cybersecurity.[162]

The efforts to get the FERC more involved in pipeline cybersecurity make sense. After all, the pipeline is interdependent to the electric grid, the "most critical of critical infrastructures."[163] In addition, the FERC is an independent agency that is better suited to deal with long-term cybersecurity issues, unlike the executive-governed TSA.[164]

All in all, the TSA does not seem the appropriate agency to regulate pipeline cybersecurity. A better approach to pipeline cybersecurity would be to empower the FERC, or a new entity under the DOE, to promulgate directives for the pipeline's cybersecurity, in the same fashion as was done with the electric sector.[165]

B. Information Sharing

One of the TSA's directives for pipeline owners and operators creates an information sharing regime, which requires that pipeline owners and operators designate a Cybersecurity Coordinator who would serve as a primary contact on

[159] PARFOMAK & JAIKARAN, *supra* note 9, at 16–17.

[160] *Id.*

[161] *See* Baksh, *supra* note 144.

[162] Energy Product Reliability Act, H.R. 6084, 117th Cong. § 2(a)(1), (3) (2021).

[163] Rebecca Kern, *Pipeline Cybersecurity Solutions Suffer from Oversight Divide*, BLOOMBERG GOV'T (June 8, 2021), https://about.bgov.com/news/pipeline-cybersecurity-solutions-suffer-from-oversight-divide/ [https://perma.cc/RQ8P-3XW7].

[164] Katherine Sauter, Comment, *Pipe Dreams: Streamlining Cybersecurity Regulatory Authority Over the Energy Industry to Increase National Security*, 72 ADMIN. L. REV. 507, 524–25 (2020).

[165] *See* Rebecca Kern, *Looming Cybersecurity Battle: Who Protects U.S. Pipelines?*, BLOOMBERG L. (June 27, 2018), https://news.bloomberglaw.com/environment-and-energy/looming-cybersecurity-battle-who-protects-u-s-pipelines-corrected?context=article-related [https://perma.cc/L3BC-4N9W].

cybersecurity matters within the pipeline entity and communicate with both the TSA and CISA.[166] The directive requires that the Cybersecurity Coordinator report to the TSA and CISA any "Cybersecurity Incident" affecting the IT or OT of the pipeline owner or operator.[167]

This model of cybersecurity regulation is referred to as "information sharing," one of the two main models of cybersecurity regulation presently.[168] While information sharing has its appeal, it is often seen as insufficient to address underlying cybersecurity issues.[169] According to Andrea Matwyshyn, both information sharing and deterrence "are not an optimal fit" for today's threats and security weaknesses.[170] Matwyshyn argues that our cybersecurity regulatory structure should take into account the "reciprocal security vulnerability" nature of most cybersecurity issues, which is "the practical reality that the information security of the private and public sector are inextricably interwoven."[171] In other words, vulnerabilities in the private sector affect the public sector, and vice versa. It is therefore impossible to isolate a cybersecurity issue to only one sector or actor.

Reciprocal security vulnerability is a concept that should guide today's pipeline cybersecurity efforts as well. Most pipeline operators or owners are private entities, the vulnerabilities of which are likely to significantly affect the public and the public sector. Information sharing is therefore not enough and should be supplemented by more comprehensive tools. For example, the federal government should share critical threat information with

[166] SD-01B, *supra* note 105, at 2.

[167] *Id.* at 2–3, 5 (defining "cybersecurity incident" as "an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).").

[168] Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1125–26 (2017) ("[T]he two dominant legal 'cybersecurity' paradigms—information sharing and deterrence—are not an ideal fit.").

[169] *Id.* at 1126–27.

[170] *Id.* at 1134.

[171] *Id.* at 1114.

the pipeline sector to fix vulnerabilities promptly and effectively.[172]

A more effective information sharing approach would be to make pipeline cybersecurity regulation more in line with polycentric governance.[173] By polycentric governance, I mean "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes."[174] In the pipeline context, this would require that pipeline operators and owners share threats, risks, and other relevant information with the other energy sector actors, and vice versa.[175] Electricity, natural gas, and oil are interrelated sectors facing similar threats.[176]

C. Overreliance on Prescriptive Standards

The TSA directive on pipeline cybersecurity measures is overly reliant on prescriptive standards, meaning that the TSA expects critical pipeline operators and owners to adopt certain specific measures to ensure the cybersecurity of their IT and OT.[177] While prescriptive standards may seem appealing in the sense that they specify in detail what measures are to be expected to ensure compliance, this approach would be stronger from a cybersecurity standpoint if it also included performance-based standards.

To achieve greater cybersecurity in the pipeline sector, the TSA must include performance standards in its directives,

[172] *See* PARFOMAK & JAIKARAN, *supra* note 9, at 18.

[173] Matwyshyn, *supra* note 168, at 1164 (describing how polycentric problems involve "balancing a large number of elements" (quoting MICHAEL POLANYI, THE LOGIC OF LIBERTY: REFLECTIONS AND REJOINDERS 193 (1951))).

[174] Jeff Kosseff, *Hacking Cybersecurity Law*, U. ILL. L. REV. 811, 848 (2020) (quoting Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 419 n.20 (2017)).

[175] *See* Suzanne Lemieux, *Protecting America's Critical Energy Infrastructure*, AM. PETRO. INST.: ENERGY TOMORROW (May 10, 2021), https://www.api.org/news-policy-and-issues/blog/2021/05/10/protecting-americas-critical-energy-infrastructure [https://perma.cc/6BP8-F6ZF] ("Many pipeline companies also participate in the Downstream Natural Gas Information Sharing and Analysis Center (ISAC) and Oil and Natural Gas ISAC as other vectors to receive and share cyber threats throughout the industry.").

[176] *See* Sauter, *supra* note 164, at 510, 515.

[177] PARFOMAK & JAIKARAN, *supra* note 9, at 16.

requiring the pipeline operators and owners to achieve certain goals while affording them the freedom to choose the means and methods to do so.[178] A performance-based standard "states requirements in terms of required results with criteria for verifying conformance, but without stating the methods for achieving required results."[179]

The use of performance-based standards in federal cybersecurity regulation is not unprecedented.[180] For example, both the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA) have performance-based cybersecurity standards in addition to prescriptive standards.[181]

V. THE PATH FORWARD: SECURING THE PIPELINE

Securing the pipeline requires addressing the shortcomings in the current regulatory approach. This part makes a list of recommendations with the view of strengthening the pipeline cybersecurity regulatory regime.

First, the TSA's role in regulating the pipeline's cybersecurity needs to be reconsidered. Primarily, the TSA's lack of expertise and staff shortage is a strong indication that another entity may be better suited to regulate and enforce pipeline cybersecurity.[182]

Second, given the increasing risk of ransomware, any pipeline cybersecurity regulation would have to be informed by the best practices and latest research on the topic. In recent years, there

[178] *See id.*

[179] Karen Scarfone et al., *Cyber Security Standards*, *in* 2 WILEY HANDBOOK OF SCIENCE AND TECHNOLOGY FOR HOMELAND SECURITY 1052, 1054 (John G. Voeller ed., 2010).

[180] *Id.*

[181] 44 U.S.C. § 3553(a)(2)(A) (requiring that federal agencies implement information security programs "consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected by an agency or on behalf of an agency"); *see* 45 C.F.R. § 164.306(d)(3) (applying a performance-based cybersecurity standard to the healthcare sector).

[182] *See, e.g.*, *Securing Our Energy Infrastructure: Legislation to Enhance Pipeline Reliability: Hearing on H.R. 6084 Before the Subcomm. on Energy of the H. Comm. on Energy and Com.*, 117th Cong. (2022) (written testimony of Richard Glick, Chairman, Federal Energy Regulatory Commission) (discussing the FERC's twelve cybersecurity standards for the energy sector as well as the FERC's suitability to regulate pipeline cybersecurity).

has been some development in the area of ransomware research that ought to be considered by pipeline cybersecurity regulators.[183]

Third, Zero Trust security is a concept that has lately become popular with entities wishing to defend against ransomware attacks. The Cybersecurity Executive Order signed by President Biden reflects the growing recognition of Zero Trust security as a tool for cybersecurity.[184]

Fourth, the reliance on prescriptive standards alone is not a panacea and is likely to be insufficient. Performance-based standards are a much-needed component to any cybersecurity regulation for the pipeline sector.

Fifth, given the current emergency authorization used to justify the two TSA directives, a more transparent and inclusive process is essential to ensure the legitimacy and efficiency of pipeline cybersecurity regulation.

Sixth, strengthening critical infrastructure cybersecurity as a whole should be part of any cybersecurity policy, which the pipeline would also benefit from.

Finally, dealing with the pipeline cybersecurity cannot only be achieved by enacting domestic regulations and passing laws. An international cooperation is vital to assure pipeline cybersecurity.[185] This involves the due diligence principles and pressuring governments to prosecute computer crimes pertaining to critical infrastructure generally and the pipeline specifically.

A. *Authorize the Department of Energy to Regulate Pipeline Cybersecurity*

Whether the TSA is the appropriate agency to regulate pipeline cybersecurity is a question that will ultimately be decided by Congress.[186] It may be the case that Congress would decide to

[183] *See, e.g.*, WILLIAM C. BARKER ET AL., NAT'L INST. STANDARDS & TECH., NISTIR 8374, RANSOMWARE RISK MANAGEMENT: A CYBERSECURITY FRAMEWORK PROFILE (2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf [https://perma.cc/XL7Q-RYKJ].

[184] Exec. Order No. 14,028, 86 Fed. Reg. 26636 (May 17, 2021).

[185] 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. 319, 343 (2013) (discussing the importance of international cooperation on cybercrime).

[186] *See* Eric Geller, *'TSA Has Screwed This Up': Pipeline Cyber Rules Hitting Major Hurdles*, POLITICO (Mar. 17, 2022, 1:45 PM), https://www.politico.com/news/2022/03/17/tsa-has-screwed-this-up-pipeline-cyber-rules-hitting-major-hurdles-00017893 [https://perma.c

fund the TSA and ensure it has the requisite expertise and human capital to effectively regulate pipeline cybersecurity. However, there is currently an ongoing debate as to whether there is a more appropriate agency that could be tasked to regulate pipeline cybersecurity. Notably, this debate predates the Colonial Pipeline ransomware attack.[187]

As the debate stands, there are currently four approaches. First, that the FERC itself regulate pipeline cybersecurity.[188] This could be achieved by reinterpreting the National Gas Act to be read as empowering the FERC with jurisdiction over "the transportation of natural gas in interstate commerce."[189] This will effectively transfer the pipeline security from the TSA to the DOE.

Second, that the FERC certify a new entity, the Energy Product Reliability Organization (EPRO), to regulate pipeline cybersecurity.[190] Under the proposed Energy Product Reliability Act, the new EPRO will create standards and enforce them against pipeline owners and operators.[191] This approach seeks to refocus the TSA's authority on physical security, while creating a new entity that will be exclusively tasked to regulate pipeline cybersecurity.[192]

Third, that CISA, instead of the TSA, regulate pipeline cybersecurity. [193] The argument goes that CISA is already overseeing sixteen critical infrastructure sectors.[194] Though it is

c/7SFG-UJX3] ("Frustration with the TSA's pipeline security efforts has reached Congress. Last year, the leaders of the House Energy and Commerce Committee proposed bipartisan legislation shifting pipeline cyber oversight to the Energy Department.").

[187] Mark Rockwell, *TSA's Role in Pipeline Cybersecurity Could Be Up for Grabs*, FCW (Sept. 27, 2018), https://fcw.com/it-modernization/2018/09/tsas-role-in-pipeline-cybersecurity-could-be-up-for-grabs/196386/ [https://perma.cc/N4AC-BVPT]; PAUL PARFOMAK, CONG. RSCH. SERV., IN11060, PIPELINE SECURITY: HOMELAND SECURITY ISSUES IN THE 116TH CONGRESS 3 (2019) [hereinafter PARFOMAK, PIPELINE SECURITY] ("[O]thers have questioned whether any of TSA's regulatory authority over pipeline security should move to another agency, such as the DOE, DOT, or FERC, which they believe could be better positioned to execute it.").

[188] Sauter, *supra* note 164, at 523 ("[T]he Commission should reinterpret the scope of its authority under the NGA.").

[189] 15 U.S.C. § 717(b).

[190] Energy Product Reliability Act, H.R. 6084, 117th Cong. § 2(d) (2021).

[191] *Id.* § 2(b).

[192] Baksh, *supra* note 144; Energy Product Reliability Act, H.R. 6084, 117th Cong. § 2(e) (2021).

[193] Elizabeth Hoffman, *TSA Should Relinquish Oversight of Pipeline Security*, CTR. FOR STRATEGIC & INT'L STUD. (June 10, 2021), https://www.csis.org/analysis/tsa-should-relinquish-oversight-pipeline-security [https://perma.cc/57SP-ZKFQ].

[194] *Id.*

not clear if CISA has the capacity to address the intricacies of the oil and gas pipeline sector.

While the proposals may seem different, they are getting at the same point, which is that the TSA is not currently capable of effectively regulating pipeline cybersecurity. The alternative is letting the DOE take the TSA's place. First and foremost, the DOE may be better suited to fulfill this task, as its energy sector's cybersecurity regulation has always been mandatory in nature.[195] This has not been the case in the pipeline context.

Second, the interdependency between the electric power sector and the pipeline cannot be overstated. Increasingly, the electric power sector is reliant upon natural gas, meaning that any vulnerabilities in the pipelines' systems will significantly affect the electric power sector.[196] Any vulnerabilities affecting the pipeline will in turn affect the energy sector as a whole, and vice versa.[197] For example, pipeline pumping stations are dependent upon a reliable source of electricity. Any cybersecurity incident affecting electricity supply will also hinder the pipeline's ability to perform its role.[198]

For example, "natural-gas-fired electric generators are directly connected to a natural gas pipeline, which supplies the generator with natural gas," which, if compromised, would affect the electricity sector as a whole.[199] These reciprocal security vulnerabilities should be addressed by allowing the FERC to regulate the pipeline's cybersecurity while letting the TSA regulate the physical security of pipelines.[200]

[195] *See* Dancy & Dancy, *supra* note 10, at 597–99.

[196] PARFOMAK, *supra* note 187 ("A 2017 Department of Energy (DOE) staff report highlighted the electric power sector's growing reliance upon natural gas-fired generation and, as a result, security vulnerabilities associated with pipeline gas supplies.").

[197] *See, e.g.*, Mark Tarallo, *Is Pipeline Security Adequate?*, ASIS INT'L (Oct. 1, 2019), https://www.asisonline.org/security-management-magazine/articles/2019/10/is-pipeline-security-adequate/ [https://perma.cc/P5PP-S6L4].

[198] DEP'T HOMELAND SEC. & DEP'T ENERGY, ENERGY: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (REDACTED) 17 (2007), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_Public.pdf [https://perma.cc/M9M5-CN9C] ("There are also interdependencies within the energy infrastructure itself, particularly the dependence of petroleum refineries and pipeline pumping stations on a reliable electricity supply and backup generators and utility maintenance vehicles to be supplied with diesel and gasoline fuel.").

[199] Sauter, *supra* note 164, at 512 ("Thus, an attack that disrupts natural gas service or its transmission could have devastating effects on electric generation and the grid.").

[200] *Id.* at 509, 524, 527.

However, the energy sector's cybersecurity regulations are not without criticism.[201] Yet, the expertise and record of the FERC may prove useful in the pipeline context, and the appropriate revisions to its authority may result in a better form of cybersecurity regulation for the pipeline sector.

There have been some proposals to include other agencies and entities in different aspects of pipeline cybersecurity. Recently proposed bills have included a proposal to authorize the Secretary of Energy to perform a certain role in pipeline cybersecurity,[202] a proposal to require that the FERC consult with the TSA on cybersecurity and interstate gas pipeline permit applications,[203] and other bills empowering the DOE,[204] U.S. Coast Guard and NIST,[205] and the Pipeline and Hazardous Materials Safety Administration[206] to also have respective roles in pipeline cybersecurity. These overlapping authorities may be cause for concern if they result in conflicting or confusing guidance.[207]

Overall, it appears that the TSA should either have some pipeline cybersecurity authority or none at all. Unless the TSA is sufficiently funded and staffed, these proposals seem likely to prevail in the future.

B. Address the Ransomware Problem

Ransomware presents a concerning risk to the pipeline. Ransomware is a malicious software that encrypts valuable data, such as medical data, barring access to it until a ransom is paid to

[201] U.S. GOV'T ACCOUNTABILITY OFF., GAO-11-117, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 22–25 (2011) (claiming that the regulations favor industry interests rather than overall cybersecurity).

[202] Pipeline and LNG Facility Cybersecurity Preparedness Act, H.R. 3078, 117th Cong. § 2 (2021).

[203] Promoting Interagency Coordination for Review of Natural Gas Pipelines Act, H.R. 1616, 117th Cong. § 3 (2021).

[204] Fixing America's Surface Transportation Act of 2015, Pub. L. No. 114–94, 129 Stat. 1312 (codified in scattered sections of 12 U.S.C., 16 U.S.C., 23 U.S.C., 40 U.S.C., 42 U.S.C., and 49 U.S.C.).

[205] U.S. COAST GUARD, MARITIME BULK LIQUID TRANSFER CYBERSECURITY FRAMEWORK PROFILE (2016), https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime_BLT_CSF.pdf?ver=2017-07-19-070544-223 [https://perma.cc/55DX-PNAA].

[206] *See, e.g.*, Protecting Our Infrastructure of Pipelines and Enhancing Safety Act of 2020, 49 U.S.C. §§ 60142, 60143, 60303.

[207] Hellmann, *supra* note 18, at 176.

the attackers.[208] Hospitals,[209] schools,[210] newspapers,[211] cities,[212] and even law enforcement[213] have become valuable targets for hackers looking for a quick monetary gain, usually in the form of untraceable cryptocurrency payouts by the victims.[214] Colonial Pipeline, who suffered a ransomware attack, had to shut down its network temporarily, impacting gasoline availability and prices, before it was left with no choice but to pay a ransom of over $4 million worth of Bitcoin.[215] Reportedly, the Department of Justice was able to recover $2.3 million worth of Bitcoin paid by Colonial Pipeline to the hackers.[216] Even in cases where victims are somehow fortunate to forgo paying the hackers, they are still likely to be spending large amounts of money and time to recover and

[208] *Ransomware and Malware*, U.S. ARMY CYBER COMMAND (Sept. 1, 2022), https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2059048/ransomware-and-malware [https://perma.cc/AX2F-ETMC] ("Ransomware is a type of malicious software, or malware, designed to deny a user access to a computer system or computer files until a ransom, typically cryptocurrency, has been paid."). Ransomware typically spreads through phishing e-mails or by unknowingly visiting an infected website. *Id.*

[209] Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ [https://perma.cc/VG27-7MAD].

[210] Nicholas Bogel-Burroughs, *Hackers' Latest Target: School Districts*, N.Y. TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html [https://perma.cc/KQ67-4TY2].

[211] Malena Carollo, *Tampa Bay Times Hit by Ransomware Attack*, TAMPA BAY TIMES (Jan. 23, 2020), https://www.tampabay.com/news/business/2020/01/23/tampa-bay-times-hit-by-ransomware-attack/ [https://perma.cc/7T89-A3LR].

[212] Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare*, WIRED (Apr. 23, 2018, 8:55 PM), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ [https://perma.cc/Q5ZG-4WMV].

[213] Chris Francescani, *Ransomware Hackers Blackmail U.S. Police Departments*, NBC NEWS (Apr. 26, 2016, 5:53 AM), https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746 [https://perma.cc/QQK4-M6K5].

[214] Michael Baker, *How Cryptocurrencies Are Fueling Ransomware Attacks and Other Cybercrimes*, FORBES TECH. COUNCIL (Aug. 3, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/?sh=662436e33c15 [https://perma.cc/TJV2-SHKF].

[215] Nicole Perlroth, *Colonial Pipeline Paid 75 Bitcoin, or Roughly $5 Million, to Hackers*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html [https://perma.cc/ZSZ2-UFCC].

[216] Christopher Bing et al., *U.S. Seizes $2.3 Mln in Bitcoin Paid to Colonial Pipeline Hackers*, REUTERS, June 7, 2021, 7:14 PM, https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/ [https://perma.cc/E2X2-KBSY].

improve the security of their systems to thwart any future ransomware.[217]

Needless to say, a ransomware attack is a criminal offense under both the Computer Fraud and Abuse Act and the federal Wire Fraud Statute.[218] However, there is little guidance as to how a victim of ransomware is to best respond to minimize the damage of a ransomware attack.[219] In the context of the pipeline, paying the ransom to release the systems and resume operations is a significant dilemma. On the one hand, consumers and the economy as a whole experience the effects of the attack against the pipeline, which incurs major costs.[220] After all, Colonial Pipeline is responsible for 45% of the fuel supplied to the East Coast, and any further disruption would have caused substantial damage to the economy.[221] On this point, Anne Neuberger, the White House Deputy National Security Advisor for Cyber and Emerging Technology, acknowledged that it is "sometimes not a feasible option for companies to decline payment, especially those that don't have backup files or other means of recovering data."[222]

On the other hand, paying the ransom does not ensure the release of the infected systems, and it further emboldens hackers to continue attacking critical infrastructure systems with

[217] Henry L. Davis, *$10 Million Cyber Attack Hits New York Hospital*, MAUREEN DATA SYS. (Feb. 13, 2018), https://www.mdsny.com/ten-million-cyber-attack-hits-new-york-hospital/ [https://perma.cc/2D93-2THJ].

[218] PETER G. BERRIS & JONATHAN M. GAFFNEY, CONG. RSCH. SERV., R46932, RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY 3–4 (2021); 18 U.S.C. § 1030(a)(7)(C); Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public [https://perma.cc/3XH9-MPEQ]; Press Release, U.S. Dep't of Just., Latvian National Charged for Alleged Role in Transnational Cybercrime Organization (June 4, 2021), https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization [https://perma.cc/WWT2-FPVF].

[219] *See* BERRIS & GAFNEY, *supra* note 222 ("[V]ictims face more nuanced legal issues when deciding whether to make ransomware payments.").

[220] *See, e.g.*, Andrea Vittorio, *Colonial Pipeline Rejects Responsibility for Hack's Gas Pump Hit*, BLOOMBERG L. (Sept. 21, 2021, 11:07 AM), https://news.bloomberglaw.com/privacy-and-data-security/colonial-pipeline-rejects-responsibility-for-hacks-gas-pump-hit [https://perma.cc/74NJ-BL7P] (reporting that consumers filed a lawsuit for having to pay higher prices for gas due to the Colonial Pipeline ransomware attack).

[221] Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, WALL ST. J. (May 19, 2021, 4:51 PM), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 [https://perma.cc/HT36-272J].

[222] *Id.*

ransomware.[223] The official FBI stance is that victims should not pay ransom.[224]

To address the ransomware problem, one must realize that it is a preventable problem. First of all, many precautions may be taken to reduce the likelihood of ransomware. For example, multifactor authentication, segmentation of networks, [225] and routine patching of systems.[226] Though patching should be done in a way that does not cause more harm than good, and system operators must evaluate whether patching is warranted or if there are other mitigation tools available.[227]

Some other recent work on ransomware, such as the Ransomware Task Force Report commissioned by the Institute for Security & Technology (IST), is an example of a comprehensive approach to address the problem.[228] The Ransomware Task Force Report lays out steps to mitigate the ransomware problem, such as international coordination, cyber insurance coverage, to target the infrastructure used by hackers, and more.[229] As long as pipeline operators and owners follow the latest research on ransomware, they may be able to protect themselves from any future attacks.

[223] *See* Newman, *supra* note 4.

[224] *Ransomware*, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware [https://perma.cc/43HQ-VDBD] (last visited Oct. 22, 2022) ("The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.").

[225] Mary K. Pratt, *What Is Zero Trust? A Model for More Effective Security*, CSO (Jan. 16, 2018, 3:08 AM), https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-moreeffective-security.html [https://perma.cc/PT9V-STBZ].

[226] Hon. Joe R. Reeder & Tommy Hall, *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, 6 CYBER DEF. REV., Summer 2021, at 20.

[227] Aaron Schaffer & Ellen Nakashima, *New Emergency Cyber Regulations Lay Out 'Urgently Needed' Rules for Pipelines but Draw Mixed Reviews*, WASH. POST (Oct. 3, 2021), https://www.washingtonpost.com/national-security/cybersecurity-energy-pipelines-ransomware/2021/10/03/6df9cab2-2157-11ec-8200-5e3fd4c49f5e_story.html [https://perma.cc/KA9U-FQV2] ("When you're dealing with an operational technology system, sometimes a patch doesn't reduce the risk or even fix the vulnerability . . . . And going down to the field in the middle of winter to take down a system to patch it can backfire. We've seen more accidental shutdowns from well-intentioned operators patching systems than were caused by attacks from Russia and Iran combined." (quoting Robert M. Lee, chief executive of Dragos, an industry cybersecurity firm)).

[228] INST. FOR SEC. & TECH., A COMPREHENSIVE FRAMEWORK FOR ACTION: KEY RECOMMENDATIONS FROM THE RANSOMWARE TASK FORCE 19 (2021), https://securityandtechnology.org/ransomwaretaskforce/ [https://perma.cc/L5P8-FAYL].

[229] *Id.* at 19, 52–53.

C. Implement Zero Trust Security Controls

In order to modernize the computer systems and networks controlling the pipeline, employees and contractors need to be limited in the kind of applications that they may run on the pipeline's IT and OT.[230] As the name suggests, Zero Trust is an approach whereby the computer systems and networks are set to not trust anything inside or outside its perimeters.[231] As such, Zero Trust is a potent tool to address the threat of ransomware attacks, as it treats each application, machine, and user as its own independent perimeter.[232] Any pipeline cybersecurity standards should implement requirements focused around Zero Trust security.

Zero Trust may prove effective in the oil and gas context, as oil and gas pipeline operators and owners are running a mix of legacy and modern systems and are generally moving slowly on digital transformation and modernization.[233]

Zero Trust has been included in the recent Cybersecurity Executive Order signed by President Biden.[234] The Cybersecurity Executive Order calls on the federal government to overhaul security by implementing Zero Trust security.[235] It also points out that the private sector should follow the government's lead. In addition, the Cybersecurity Executive Order addresses some of the shortcomings in the current cybersecurity approach to the energy sector. Just like the TSA directive, the Executive Order removes barriers to information sharing between the private sector and the government.[236] It also improves software supply chain security,

[230] *See, e.g.*, MICROSOFT, EVOLVING ZERO TRUST 3, 5 (2021), https://www.microsoft.com/en-us/security/business/zero-trust [https://perma.cc/B3BE-NTRQ].

[231] Pratt, *supra* note 225.

[232] Scott Matteson, *How to Prevent Ransomware Attacks with a Zero-Trust Security Model*, TECH REPUBLIC (July 9, 2021, 9:43 AM), https://www.techrepublic.com/article/how-to-prevent-ransomware-attacks-with-a-zero-trust-security-model/ [https://perma.cc/QAY5-5JE4].

[233] *Id.* ("[Z]ero trust is especially crucial for companies in industries that have been slower to modernize, such as oil and gas, utilities, and energy. Due to their delayed digital transformation, as well as a mix of legacy and modern equipment, these companies are often the most difficult to secure.").

[234] Exec. Order No. 14,028, 86 Fed. Reg. 26635–36 (May 17, 2021).

[235] MeriTalk Staff, *Colonial Pipeline Hack Rockets Ransomware to Top of U.S. Security Agenda*, MERITALK (June 30, 2021, 9:05 AM), https://www.meritalk.com/articles/critical-infrastructure-special-report/ [https://perma.cc/2SHR-6J6B].

[236] Exec. Order No. 14,028, 86 Fed. Reg. 26633 (May 17, 2021).

establishes a cybersecurity safety review board, and creates a standard playbook for cybersecurity incident response.[237]

D. Rely on Performance-Based Standards for Pipeline Cybersecurity

The emerging body of pipeline cybersecurity regulation will have to find the appropriate balance between the current TSA approach of prescriptive standards and the more preferable approach, performance-based standards.[238] The performance-based approach would create objectives for pipeline owners and operators to strive for as they design their cybersecurity systems, methods, and processes.[239]

Prescriptive standards are often seen as rigid and can quickly become outdated if they cannot keep up with evolving practices and risks.[240] This does not automatically suggest that these standards are without utility but that they must be supplemented by additional means.

The performance-based standards approach was at the center of the Obama Administration's Improving Critical Infrastructure Cybersecurity Executive Order.[241] This Executive Order tasked NIST to create a voluntary cybersecurity framework for the critical infrastructure that is "prioritized, flexible, repeatable, performance-based, and cost-effective."[242] It is also at the core of the Biden Administration's policy for the critical infrastructure, where both the DHS and NIST were tasked to develop

[237] Claudia Rast, *The Continuing Cybersecurity Threat to U.S. Energy Infrastructure*, ABA SECTION ENV'T, ENERGY & RES.: TRENDS (Sept. 8, 2021), https://www.americanbar.org/groups/environment_energy_resources/publications/trends/2021-2022/september-october-2021/the-continuing-cybersecurity/ [https://perma.cc/N9NW-BYKV].

[238] Nakashima & Aratani, *supra* note 145 (noting that under the performance-based approach, "[t]he idea is to specify key objectives for the company, allowing it to innovate and keep up with technology to accomplish the goals, experts said").

[239] *Id.*

[240] Jonathan Greig, *Security Experts Question New DHS/TSA Cybersecurity Rules for Rail Companies*, ZDNET (Dec. 6, 2021), https://www.zdnet.com/article/security-experts-question-new-dhstsa-cybersecurity-rules-for-rail-companies/ [https://perma.cc/7N39-Y24F] (noting that prescriptive standards would "limit affected industries' ability to respond to evolving threats, thereby lessening security").

[241] Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11741 (Feb. 12, 2013).

[242] *Id.* at 11740–41; Dan Lips, *How Congress and NIST Can Help Organizations Better Manage Cyber Risk*, LAWFARE (Aug. 31, 2021, 8:48 AM), https://www.lawfareblog.com/how-congress-and-nist-can-help-organizations-better-manage-cyber-risk [https://perma.cc/2RQR-SQT7].

"cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security."[243]

Setting performance-based standards for the pipeline sector is likely to enhance the overall security of its systems, networks, and data. This is similar to what Jeff Kosseff referred to as "adaptive" cybersecurity law.[244] However, there is some industry pushback against performance-based standards, as they are often deemed to be burdensome and costly.[245] A reasonable and effective balance between the prescriptive and performance-based standards will have to be struck by the regulating agency.

E. Increase Transparency in Pipeline Cybersecurity

The two TSA cybersecurity directives have drawn some criticism due to the nontransparent nature of the emergency rulemaking authority supporting their creation.[246] The government promulgating regulations in emergency situations is not without merit,[247] yet transparency and stakeholder inclusion should also be accounted for. As a result of this process, experts and industry stakeholders have not been adequately consulted regarding the two directives. A letter to the DHS Inspector General from two ranking members on the Committee on Homeland Security & Governmental Affairs, James Lankford and Rob Portman, as well as Senator Michael Rounds, has expressed some of that concern. According to the letter, "securing critical infrastructure requires a collaborative approach with the experts in these industries—the

[243] Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, 2021 DAILY COMP. PRES. DOC. 1–2 (July 28, 2021).

[244] Kosseff, *supra* note 174, at 828.

[245] Lips, *supra* note 242 ("Counterarguments to an increased regulatory approach will likely include that the compliance burden of new regulations will be costly and counterproductive.").

[246] Kirstin Gibbs & Arjun Prasad Ramadevanahalli, *Emergency Cybersecurity Regulations in the Pipeline Industry: Unique Challenges and Opportunities Ahead*, JD SUPRA (Dec. 20, 2021), https://www.jdsupra.com/legalnews/emergency-cybersecurity-regulations-in-6021339/ [https://perma.cc/2SLQ-EPUS] ("TSA released SD2 pursuant to its statutory emergency authority, which allows the agency to issue regulations without the opportunity for notice and comment if needed 'to protect transportation security.'" (quoting 49 U.S.C. § 114(l)(2)(A))).

[247] Zhang, *supra* note 185, at 341 ("Allowing the federal government to have emergency powers to address immediate and pending threats would utilize its strengths.").

people who operate this critical infrastructure and who are charged with implementing these directives."[248]

Similarly, pipeline trade associations have laid out the same concerns in their letter to the TSA Administrator, David Pekoske.[249] According to the letter, the directives may cause disruptions in the oil and gas sector, which "conveyed highly probable operational safety and reliability concerns that could arise by imposing prescriptive cyber requirements and untenable timelines without specific understanding of a company's existing cybersecurity protections and operations."[250]

These concerns could be alleviated if the TSA were to consult the relevant industry stakeholders and experts in a normal notice-and-comment rulemaking process. Experts equally support the development of pipeline cybersecurity regulations through a transparent and collaborative process, which would in turn create more effective regulation altogether.[251]

Congress is attempting to address some of these concerns. In the recently proposed Pipeline Security Act, requiring the TSA to "convene not less than two industry days to engage with relevant pipeline transportation and pipeline facilities stakeholders on matters related to the security of pipeline transportation and pipeline facilities."[252] Any future cybersecurity directives will have to involve substantive input from the industry to enhance legitimacy and efficiency.

F. Strengthen the Critical Infrastructure's Cybersecurity

Pipeline is but one part of the overall U.S. critical infrastructure, though there is some debate as to what exactly falls under the scope of critical infrastructure.[253] Any policy to ensure

[248] Letter to Joseph Cuffari, *supra* note 146.

[249] Letter from AFPM, AGA, AOPL, API, APGA, INGAA, and GPA Midstream to David P. Pekoske, Adm'r, Transp. Sec. Admin. (Aug. 24, 2021) [hereinafter Industry Letter to Administrator Pekoske], *reprinted in* Letter from Rob Portman, James Lankford, and M. Michael Rounds to Joseph V. Cuffari, Inspector General, Dep't Homeland Sec. (Oct. 28, 2021).

[250] Industry Letter to Administrator Pekoske, *supra* note 249.

[251] Schaffer & Nakashima, *supra* note 227.

[252] Pipeline Security Act of 2021, H.R. 3243, 117th Cong. § 6 (2021).

[253] Tasha Jhangiani & Graham Kennis, *Protecting the Critical of Critical: What Is Systemically Important Critical Infrastructure?*, LAWFARE (June 15, 2021, 12:02 PM), https://www.lawfareblog.com/protecting-critical-critical-what-systemically-important-critical-i

the cybersecurity of the pipeline will have to also include the bigger picture of the U.S. critical infrastructure system as a whole. Around 85% of U.S. critical infrastructure is privately owned, so any regulation or policy pertaining to critical infrastructure cybersecurity will have to heavily focus on the private sector.[254] However, there is some disagreement as to who exactly should defend critical infrastructure when both the public and private sector are so intertwined in it.[255]

On July 28, 2021, President Biden released the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.[256] This memorandum directs the Secretaries of Homeland Security and Commerce (through CISA and NIST) to develop and issue performance goals for critical infrastructure owners and operators to follow regarding cybersecurity.[257]

The allocation of cyber defense responsibilities is crucial for the improvement of the critical infrastructure's overall cybersecurity.[258] Though, in all scenarios, both the private sector and the government would have to engage in the protection of the critical infrastructure.[259] This is due to the reciprocal security vulnerability problem and other concerns.[260] In the words of Andrea Matwyshyn: "[S]mart grids, power and water stations, air traffic control systems and other communication systems, health systems, and nuclear power plants—all blend private and public-sector elements."[261]

nfrastructure [https://perma.cc/DXJ5-YK8T] ("The U.S. government is not completely aware of *what* is critical . . . the term 'critical infrastructure' has grown so large that it has lost any meaningful specificity.").

[254] Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 494 (2017).

[255] *Id.* at 495 ("In the last few years, the federal government and the private sector have exhibited contradictory views about who should defend the networks.").

[256] Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, *supra* note 243.

[257] *See id.*

[258] Zhang, *supra* note 185, at 332, 336 (discussing the "[u]nclear [a]ssignment of [r]esponsibility" in the context of cybersecurity incidents against the electricity sector).

[259] *See id.* at 336 ("Responsibility for cybersecurity should shift between the government and the private industry depending on timing and the circumstances of the cyber event.").

[260] Matwyshyn, *supra* note 168, at 1121.

[261] *Id.* at 1121–22 (footnotes omitted).

Both the Executive Order on Improving Critical Infrastructure Cybersecurity[262] and the Presidential Policy Directive-21: Critical Infrastructure Security and Resilience[263] will need to further implement lessons from information security, which includes best practices to tackle the ransomware problem and new methodologies like Zero Trust security. The strengthening of all critical infrastructure, which often has overlapping vulnerabilities, threats, and risks, will in turn enhance the cybersecurity of the pipeline.

G. Set an International Due Diligence Standard

The reality of foreign cyberattacks against U.S. pipelines may not be addressed solely through U.S. domestic laws and regulations. To prevent and respond to foreign cyberattacks, foreign governments should have some form of due diligence[264] to make sure that cyberattacks are not carried out against another nation's infrastructure and, if they are, that the perpetrators are prosecuted.[265]

President Biden has made remarks to the same effect. In the immediate aftermath of the Colonial Pipeline ransomware attack, President Biden suggested that the international community will need to develop an "international standard" pertaining to state responsibility for harmful cyberattacks originating in their territory.[266] Accordingly, "if the Russian government knew the identity and location of DarkSide," the hacking group responsible for Colonial Pipeline, then the Russian government "would have

[262] Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

[263] Directive on Critical Infrastructure Security and Resilience, 1 PUB. PAPERS 106 (Feb. 12, 2013).

[264] *See, e.g.*, Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 TEX. L. REV. 1555, 1566–67 (2017) ("A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." (quoting TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 30 (Michael N. Schmitt & Liis Vihul eds., 2017))).

[265] *See* Miller, *supra* note 79 (reporting that Russia arrested the Colonial Pipeline hackers and is expected to prosecute them).

[266] Remarks on the Colonial Pipeline Ransomware Attack and an Exchange with Reporters, 2021 DAILY COMP. PRES. DOC. 1, 3 (May 13, 2021).

been obliged to take all feasible measures to put an end to the Colonial Pipeline operation."[267]

Beyond due diligence, dealing with the international character of ransomware attacks against critical infrastructure requires "international diplomatic and law enforcement efforts . . . to direct nation-states away from providing safe havens to ransomware" hackers.[268] This is a step to address ransomware more broadly, as the pipeline is by far not the only target of hackers using ransomware.[269]

VI. CONCLUSION

Pipeline cybersecurity is a complex topic that involves a multitude of competing interests and regulatory entities. There have been many developments with regard to pipeline cybersecurity in the aftermath of the Colonial Pipeline ransomware attack of 2021, including the issuance of new directives by the TSA. These directives also represent a shift from a voluntary guidance approach to mandatory directives to shape the pipeline's cybersecurity methods, procedures, and information sharing. However, the process is incomplete, and many open questions remain.

First and foremost, it does not appear that the TSA is the appropriate or most effective agency to tackle the thorny problem of the cybersecurity risks that pipeline operators and owners face. The TSA lacks the requisite expertise to take on the pipeline cybersecurity role and the staff necessary to carry out such role. Some proposals have been made to empower the DOE, or another third party, to handle pipeline cybersecurity. The current Administration seems very much in support of this alternative. This is the correct path forward, though some challenges with the DOE may need to be resolved before it is to regulate the pipeline's cybersecurity.

[267] Scott Jasper, *Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack*, ATL. COUNCIL (June 1, 2021), https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/ [https://perma.cc/4LX4-HTER].

[268] INST. FOR SEC. & TECH., *supra* note 228, at 6.

[269] *Cyberattack Impacts MTSA Facility Operations*, MARINE SAFETY INFO. BULL. (U.S. Coast Guard, D.C.), Dec. 16, 2019 (discussing the ransomware attack against the U.S. Coast Guard).

Second, the substance of any prospective pipeline cybersecurity regulation will have to take into account the latest research on ransomware risk management and response, as well as Zero Trust security and other potential methods of protecting the pipeline infrastructure against cyberattacks. It will also have to involve input from industry and information security experts to ensure legitimacy and efficiency. The current substantive approach to pipeline cybersecurity is also overly prescriptive. More performance-based standards would provide the necessary balance between the two models of cybersecurity standardization.

Third, to improve pipeline cybersecurity, the U.S. government will have to address deficiencies in its current approach to critical infrastructure cybersecurity. Primarily, the question of the cyber defense responsibilities is of increased importance. Ideally, the federal government should have a central role in protecting the critical infrastructure.

Finally, the international character of cyberattacks against pipeline systems requires some effort to incentivize other nations to cooperate on cybercrime enforcement. This could be achieved by an emerging due diligence principle, obligating any hacker-harboring nation to prevent cyberattacks. Recent diplomacy efforts have led to the arrest and prosecution of the fourteen hackers involved in the Colonial Pipeline ransomware attack. Future attacks, regardless of origin, should be addressed by the aggrieved nation in a similar fashion.

Pipeline cybersecurity regulation remains a priority for the U.S. government. This Article has presented some pressing issues that require resolution, as well as recommendations to respond to some of these issues. Future legislative, regulatory, and policy initiatives would do well to acknowledge these open questions, challenges, and gaps.